MODEL 7612 SNMP DSU

WITH INTERNAL ETHERNET LAN ADAPTER

USER'S GUIDE

Document No. 7612-A2-GB20-10

November 1997

PARADYNE™

Copyright © 1997 Paradyne Corporation.
All rights reserved.
Printed in U.S.A.

Notice

This publication is protected by federal copyright law. No part of this publication may be copied or distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means, electronic, mechanical, magnetic, manual or otherwise, or disclosed to third parties without the express written permission of Paradyne Corporation, 8545 126th Avenue North, P.O. Box 2826, Largo, Florida 33779-2826.

Paradyne Corporation makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Further, Paradyne Corporation reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of Paradyne Corporation to notify any person of such revision or changes.

Changes and enhancements to the product and to the information herein will be documented and issued as a new release to this manual.

Trademarks

All products and services mentioned herein are the trademarks, service marks, registered trademarks or registered service marks of their respective owners.

Warranty, Sales, and Service Information

Contact your sales or service representative directly for any help needed. For additional information concerning warranty, service, repair, spare parts, installation, documentation, or training, use one of the following methods:

- **Via the Internet:** Visit the Paradyne World Wide Web site at http://www.paradyne.com
- **Via Telephone:** Call our automated call system to receive current information via fax or to speak with a company representative.
  - — Within the U.S.A., call 1-800-870-2221
  - — International, call 727-530-2340

Printed on recycled paper

Contents

About This Guide

- Document Purpose and Intended Audience vii
- Document Summary vii
- Product-Related Documents viii

1 About the DSU

- Model 7612 SNMP DSU Features 1-1
- Typical SNMP DSU Configurations 1-3
- SNMP Management Capabilities 1-4
  - Management Information Base (MIB) Support 1-4
- Rear Panel Interface Connections 1-4

2 Using the ASCII Terminal Interface

- Accessing the ATI 2-1
  - Connecting to the Terminal Port 2-1
- Main Menu 2-2
- Screen Format Types 2-3
  - What Affects Screen Displays 2-3
  - Screen Work Areas 2-4
- Navigating the Screens 2-5
  - Keyboard Keys 2-5
  - Screen Function Keys 2-6
  - Switching to the Screen Function Key Area 2-7
- Ending an ATI Session 2-8

3 Configuring the DSU

- Entering Device and System Information 3-1
  - Device Name 3-2
  - System Fields 3-2
- Identity Information 3-3
- Configuring the DSU 3-4
  - Configuration Option Areas 3-4
  - Accessing and Displaying Configuration Options 3-5
  - Saving Configuration Options 3-6

4 Security

- Overview 4-1
  - Creating a Login 4-2
  - Deleting a Login 4-3
  - ATI Access 4-3
  - Effective Access Level 4-4
- Controlling SNMP Access 4-6
  - Assigning SNMP Community Names and Access Types 4-6
  - Limiting SNMP Access through the IP Addresses of the Managers 4-6

5 IP Addressing

- Selecting an IP Addressing Scheme 5-1
- IP Addressing Scheme Examples 5-2
  - IMC Connection – Same Subnet 5-2
  - Using Routers to Route DSU Management Data 5-3
- Assigning IP Addresses and Subnet Masks 5-4

6 Monitoring the DSU

- What to Monitor 6-1
- DSU LEDs 6-2
  - System LEDs 6-3
  - Network LEDs 6-4
  - Port LEDs 6-5
- Status Screen Commands 6-6
- System and Test Status 6-6
  - Self-Test Results 6-8
  - Test Status Messages 6-9

- Network Interface Status 6-10
- Network Performance Statistics 6-11
- Ethernet Port Status 6-12
- Management Protocol Statistics 6-13

7 Testing

- Detecting Problems 7-1
- Tests Available 7-2
- Network Tests 7-3
  - CSU or External Network Loopback 7-3
  - DSU or Internal Network Loopback 7-4
  - Send V.54 Up/Down Sequences 7-4
  - 511 Test Pattern for the Network 7-4
- Data Port Tests 7-5
  - Local Loopback 7-5
  - 511 Test Pattern for the DTE 7-5
- Lamp Test 7-6
- Ending an Active Test 7-6
- Loopbacks 7-7
- Device Reset 7-8

8 Messages and Troubleshooting

- Overview 8-1
- Configuring SNMP Traps 8-1
- Device Messages 8-2
- Troubleshooting 8-3

A Configuration Option Tables

- Overview A-1
- System Options Menu A-2
- Network Interface Options Menu A-5
- Data Port Options Menu A-7
- Ethernet Port Options Menu A-9
- Terminal Port Options A-10
- Telnet Session Options A-12
- SNMP Menu A-14
  - General SNMP Management Options A-14
  - SNMP NMS Security Options A-15
  - SNMP Traps Options A-17

B Worksheets

- Overview B-1
- Configuration Worksheets B-1

C MIB Descriptions

- Overview C-1
- MIB II – RFC 1213 and RFC 1573 . . . . . C-1
  - System Group C-2
  - Interfaces Group C-3
  - Extension to Interface Table (ifXTable) C-6
  - Interface Stack Group C-7
  - Interface Test Table C-8
  - Generic Receive Address Table C-9
  - IP Group C-10
  - ICMP Group C-12
  - TCP Group C-12
  - UDP Group C-12
  - Transmission Group C-12
  - SNMP Group C-12
- RS-232-Like MIB, RFC 1659 . . . . . C-13
  - Number of RS-232-Like Ports Object C-13
  - General Port Table Objects C-13
  - Asynchronous Port Table Objects C-14
  - Synchronous Port Table Objects C-15
  - Input Signal Table Objects C-16
  - Output Signal Table Objects C-17
- Ethernet-Like MIB, RFC 1643 . . . . . C-17
- Enterprise MIB C-17
  - Device Configuration Variable (pdn-common 7) C-18
  - DDS Interface Specific Definitions, pdn-dds (pdn-interfaces 2) C-18
  - Device Security, pdn-security (pdn-common 8) C-18
  - Device Traps, pdn-traps (pdn-common 9) C-18
  - Device Control, pdn-control (pdn-common 10) C-18

D Standards Compliance for SNMP Traps

- Overview D-1
- Trap: warmStart D-1
- Trap: authentificationFailure D-1
- Traps: linkUp and linkDown D-2
- Traps: enterpriseSpecific D-3

E Cables and Pin Assignments

- Overview E-1
- Terminal Port (EIA-232) Connector E-2
- DTE Port (V.35) Connector E-3
- Standard EIA-232-D Crossover Cable E-4
- Standard Null-Modem Cable E-5
- 10BaseT Connector E-6
- Modular RJ48S DDS Network Interface Connector E-6

F Technical Specifications

Glossary

Index

About This Guide

Document Purpose and Intended Audience

This guide contains information needed to set up, configure, and operate the Model 7612 DSU and is intended for installers and operators.

Document Summary

Section	Description
Chapter 1	*About the DSU.* Describes the DSU features and SNMP management capabilities with a typical configuration example.
Chapter 2	*Using the ASCII Terminal Interface.* Provides instructions for accessing the user interface and navigating the screens.
Chapter 3	*Configuring the DSU.* Provides procedures for establishing device and system identification and configuring the DSU.
Chapter 4	*Security.* Presents procedures for creating a login, setting the effective access levels, and controlling SNMP access.
Chapter 5	*IP Addressing.* Provides details regarding IP addresses with examples.
Chapter 6	*Monitoring the DSU.* Describes the LEDs, DSU status screens, and network statistics.
Chapter 7	*Testing.* Provides details about available tests and test setup.
Chapter 8	*Messages and Troubleshooting.* Provides information on SNMP traps, device messages, and troubleshooting.

Section	Description
Appendix A	*Configuration Option Tables.* Contains all configuration options, default settings, and possible settings.
Appendix B	*Worksheets.* Contains all the configuration options, default settings, and possible settings to use for planning.
Appendix C	*MIB Descriptions.* Provides an overview of the MIB objects supported by the DSU.
Appendix D	*Standards Compliance for SNMP Traps.* Contains SNMP trap compliance details.
Appendix E	*Cables and Pin Assignments.* Contains connector and interface details.
Appendix F	*Technical Specifications.* Contains physical and regulatory specifications, clock rates, and LADS connection distances.
Glossary	Defines acronyms and terms used in this document.
Index	Lists key terms, acronyms, concepts, and sections in alphabetical order.

Product-Related Documents

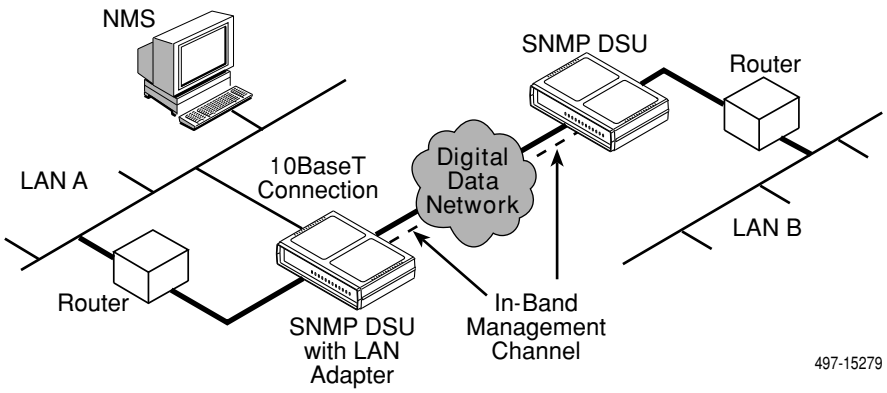
Document Number	Document Title
7612-A2-GN10	*Model 7612 SNMP DSU with Internal Ethernet LAN Adapter Startup Instructions*

To order additional product documentation, refer to *Warranty, Sales, and Service Information* on page A at the beginning of this User's Guide.

About the DSU

1

Model 7612 SNMP DSU Features



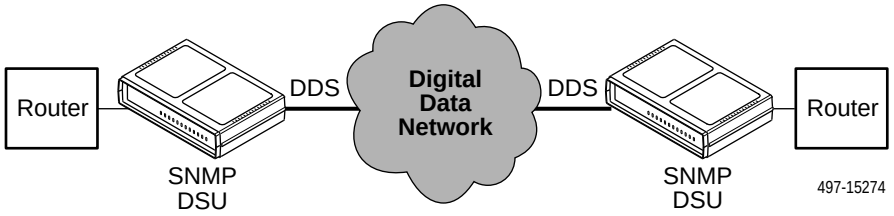
The Model 7612 SNMP DSU provides an interface between the customer premises equipment (CPE) and a DDS network. Its features include:

- **Integral LAN Adapter.** Connects the DSU directly to an Ethernet LAN.
- **SNMP (Simple Network Management Protocol) Management.** Provides network management via an industry-standard SNMP management system.
- **In-band Management Channel (IMC).** Provides remote management via SNMP or Telnet session capability over the DDS network.
- **ASCII Terminal Interface (ATI).** Provides a menu-driven VT100-compatible interface for configuring and managing the DSU locally or remotely by Telnet session or external modem.
- **Local Management.** Provides local management via an:
  - — Asynchronous terminal connection through the Terminal port
  - — NMS connection through the 10BaseT port

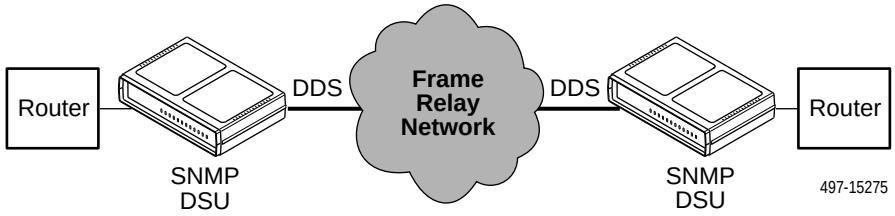
- **Remote Management.** Provides remote management:
  - — Using an external modem through the Terminal port
  - — Using SNMP or Telnet through the 10BaseT port or the IMC
- **DDS Operation.** Operates at 56 kbps and 64 kbps CC (clear channel).
- **LADS (Local Area Data Set) Operation.** Operates as a limited-distance modem at 56 kbps and 64 kbps full-duplex.
- **Autorating of Line Rate.** Establishes the line rate from the network receive signal and automatically adjusts to the detected line rate.
- **Data Port Rates.** Automatically adjusts to the DDS or LADS operating rates.
- **Diagnostics.** Provides the capability to diagnose device and network problems and perform tests, including digital loopbacks, pattern tests, and self-test.
- **Device and Test Monitoring.** Provides the capability of tracking and evaluating the unit's operation, including health and status, and error-rate monitoring.
- **Two Customer-Specified Configuration Storage Areas.** Allows quick access to alternate sets of configuration options.
- **Security.** Provides multiple levels of security, which help prevent unauthorized access to the DSU.

Typical SNMP DSU Configurations

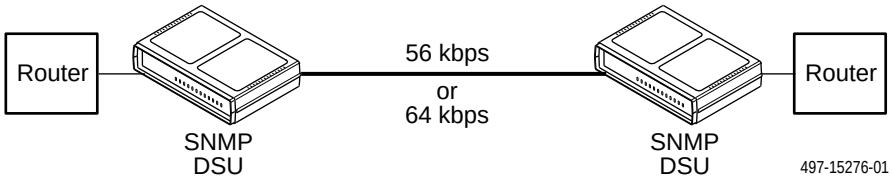
The following illustration shows a typical LAN/WAN interconnection application for the DSU. The routers connected to the DSU at each location provide the LAN interconnection.



The SNMP DSU can also be used in a frame relay network.



Two SNMP DSUs can be connected back-to-back to act as Local Area Data Sets. Table F-3 in Appendix F, *Technical Specifications*, shows the maximum distances for LADS applications.



SNMP Management Capabilities

The DSU supports SNMP Version 1, and can be managed by any industry-standard SNMP manager and accessed using SNMP by external SNMP managers.

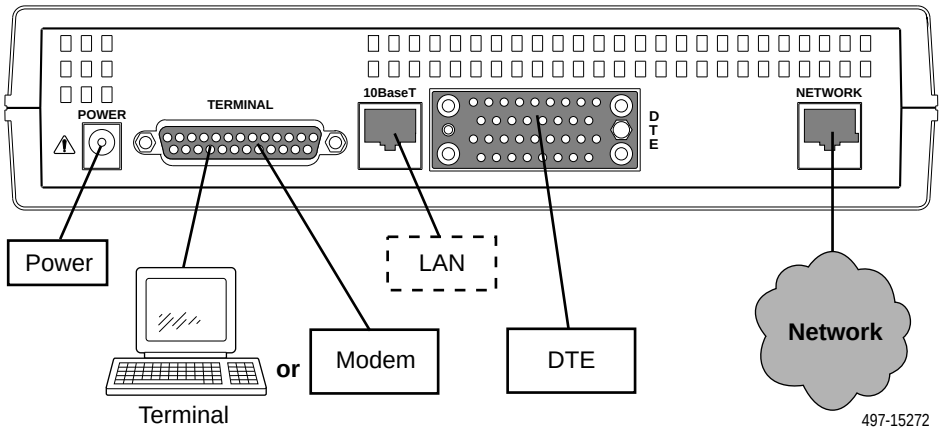
Management Information Base (MIB) Support

The following MIBs are supported:

- **MIB II (RFC 1213 and RFC 1573)** – Defines the general objects for use with a network management protocol in TCP/IP internets and provides general information about the DSU. MIB II is backward-compatible with MIB I.
- **RS-232-Like MIB (RFC 1659)** – Defines objects for managing RS-232-type interfaces (e.g., V.35, RS-422, RS-423, etc.) and supports the synchronous data port on the DSU.
- **Ethernet-like MIB (RFC 1643)** – Defines objects for managing Ethernet-like interfaces (e.g., 10BaseT).
- **Enterprise MIB** – Supports configuration, status, statistics, and tests.

Rear Panel Interface Connections

The following illustration shows the physical interfaces of the DSU. Information about the installation of the DSU is contained in the *Model 7612 SNMP DSU with Internal Ethernet LAN Adapter Startup Instructions*.



Using the ASCII Terminal Interface

2

Accessing the ATI

You can communicate with the ASCII Terminal Interface (ATI) using one of the following methods:

- Direct connection through the Terminal port.
- Dialing in through an external modem to the Terminal port.
- Telnet session through the 10BaseT port.
- Telnet session through the In-band Management Channel (IMC).

NOTE:

Only one ATI session can be active at a time, and another user's session cannot be forced to end. To automatically log out a user due to inactivity, enable the Inactivity Timeout option (see Table A-5, Terminal Port Options, and Table A-6, Telnet Session Options.

The user interface is idle until activated. Press Return to activate the user interface. Security can limit ATI access several ways. To setup security or a login ID, refer to Chapter 4, *Security*.

Connecting to the Terminal Port

Verify that the settings of the device that you connect to the Terminal port match these factory-loaded option default settings:

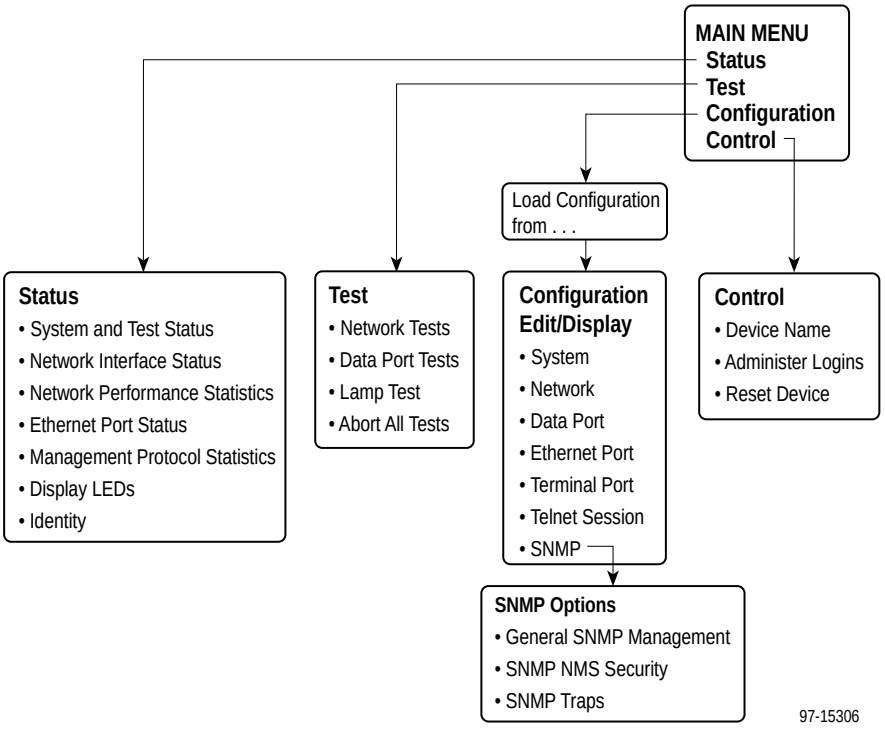
- Data rate set to 9.6 kbps.
- Character length set to 8.
- Parity set to None.
- Stop Bits set to 1.

To change the Terminal Port settings, refer to Table A-5, Terminal Port Options.

Main Menu

Entry to all of the DSU's tasks begins at the Main Menu screen, which has four menus or branches.

Select . . .	To . . .
Status	View diagnostic tests, network status of interfaces, statistics, LEDs, and DSU identity information.
Test	Select and cancel tests for the DSU's interfaces.
Configuration	Display and edit the configuration options.
Control	Control the user interface for device naming and login administration, or to initiate a power-up reset of the DSU.



Screen Format Types

Three types of screen formats are available on the ATI.

Use the screen format . . .	To . . .
Menu selection	Display a list of available functions for user selection.
Input	Add or change information on a screen. Input or edit fields that have an Underline in the field value or selection. See *Screen Work Areas* on page 2-4
Display	Display configuration information and results from performance and DSU-specific tests. Display-only fields that have no underline in the field value.

What Affects Screen Displays

What appears on the screens depends on the:

- **Current configuration** – How the DSU is currently configured.
- **Effective security access level** – An access level that is typically set by the system administrator for each interface and each user.
- **Data selection criteria** – What you entered in previous screens.

Screen Work Areas

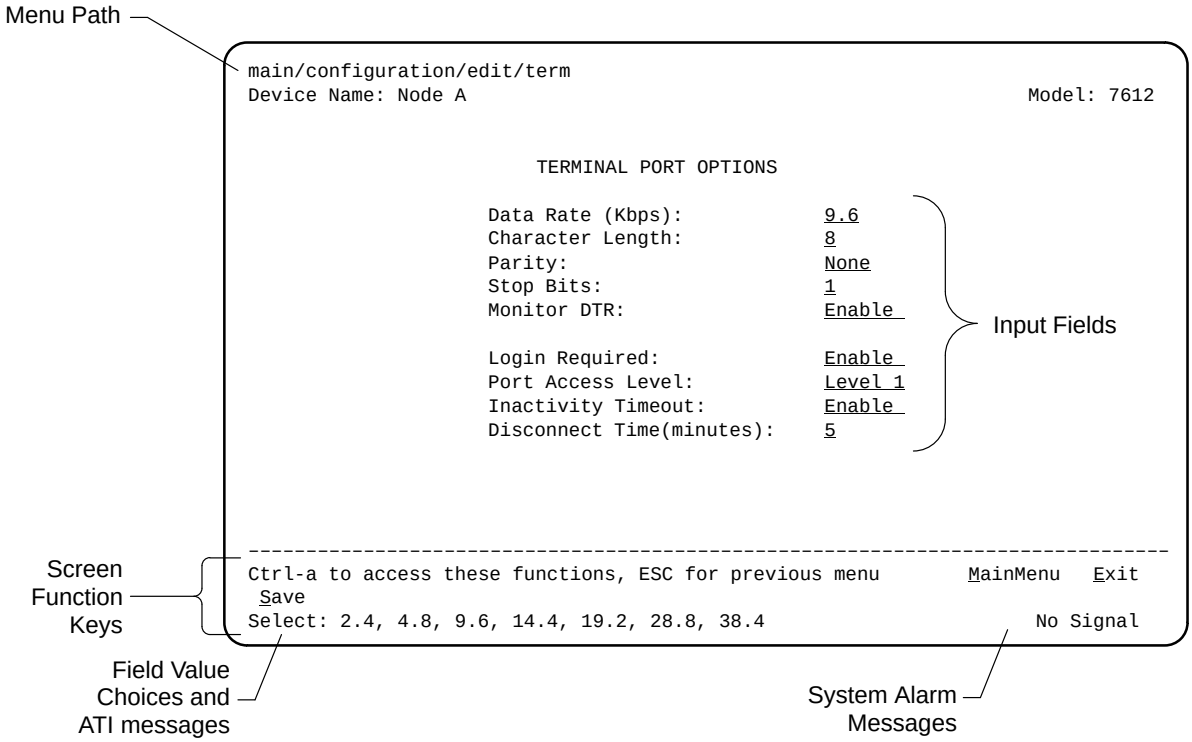
There are two user work areas:

- **Screen area** – Provides the menu path, access level, menus, and input fields above the dotted line.

  The menu path appears as the first line on the screen. In this manual, the menu path is presented as a menu selection sequence with the names of the screens:

  Main Menu → Configuration → Load Configuration From → Edit → Terminal Port

- **Screen function key area** – Provides functions available below the dotted line based upon screen selection and access level. See *Switching to the Screen Function Key Area* on page 2-7.



Navigating the Screens

You can navigate the screens by:

- Using keyboard keys
- Using screen function keys
- Switching between the two screen work areas

Keyboard Keys

Use the following keyboard keys to navigate within the screen.

To . . .	Press . . .
Move cursor between the screen area and the screen function keys area below the dotted line at the bottom of the screen	Ctrl-a
Return to the previous screen	Esc
Move cursor to the next field on the screen	Tab
Accept entry or display valid options on the last row of the screen when pressed before entering data or after entering invalid data	Return (Enter)
Move cursor one position to the left	Ctrl-k
Select the next valid value for the field	Spacebar
Delete character that the cursor is on	Delete (Del)
Move cursor up one field within a column on the same screen	Up Arrow or Ctrl-u
Move cursor down one field within a column on the same screen	Down Arrow or Ctrl-d
Move cursor one character to the right if in edit mode	Right Arrow or Ctrl-f
Move cursor one character to the left if in edit mode	Left Arrow or Ctrl-b
Redraw the screen display, clearing information typed in but not yet entered	Ctrl-l

▶ Procedure

To make a menu or field selection:

1. Press the tab key or the arrow keys to position the cursor on a menu or field selection. Each selection is highlighted as you press the key to move the cursor from position to position.
2. Press Return. The selected menu or screen appears.
3. Continue Steps 1 and 2 until you reach the screen you want.

The current setting or value appears to the right of the field name. The valid choices for the field are displayed in the screen function area. You can enter information into a selected field by typing in the first character or characters of a field value or command.

If a field is blank and the Field Values screen area displays valid selections, press the spacebar and the first valid value for the field will appear. Continue pressing the spacebar to scroll through other valid values.

Screen Function Keys

All screen function keys located below the dotted line operate the same way (upper- or lowercase) throughout the screens.

For the screen function . . .	Select . . .	And press Return to . . .
Clear	C or c	Clear status messages for one-time events.
ClrStats	C or c	Clear statistics and refresh the screen.
DeLete	L or l	Delete data.
Exit	E or e	Terminate the async terminal session.
MainMenu	M or m	Return to the Main Menu screen.
New	N or n	Enter new data.
PgDn	D or d	Display the next page.
PgUp	U or u	Display the previous page.
Refresh	R or r	Update screen with current information.
ResetMon	R or r	Reset an active Monitor 511 test counter to zero.
Save	S or s	Save information.

Switching to the Screen Function Key Area

Selecting Ctrl-a allows you to switch between the two screen work areas to perform all screen functions.

▶ Procedure

To access the screen function area below the dotted line:

1. Press Ctrl-a to switch from the screen area to the screen function key area below the dotted line. The available selections for the first input field appear on the last line as shown below.
2. Select either the function's designated (underlined) character or press the tab key until you reach the desired function key.

   Example:
   To save the changes you have made on this screen, enter s or S (Save).
3. Press Return. The function is performed.
4. To return to the screen area above the dotted line, press Ctrl-a again.

```
main/configuration/edit/term
Device Name: Node A                                          Model: 7612


                        TERMINAL PORT OPTIONS

                    Data Rate (Kbps):           9.6
                    Character Length:           8
                    Parity:                     None
                    Stop Bits:                  1
                    Monitor DTR:                Enable

                    Login Required:             Enable
                    Port Access Level:          Level 1
                    Inactivity Timeout:         Enable
                    Disconnect Time(minutes):   5



--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu   Exit
 Save
```

Ending an ATI Session

Use the Exit function key from any screen to terminate the session.

▶ Procedure

To end an ATI session:

1. Press Ctrl-a to go to the screen function key area below the dotted line.
2. Save changes if you have altered your configuration.
3. Select Exit and press Return. The User Interface Idle screen appears.

Configuring the DSU

3

Entering Device and System Information

Use the Device Name screen to input DSU device and SNMP system entries. To access the Device Name screen, follow this menu selection sequence:

Main Menu → Control → Device Name

```
main/control/device name
Device Name:                                                        Model: 7612


                                 DEVICE NAME

    Device Name:     NE815378 ________________                      Clear
    System Name:     lllQJ98-001_______________________________     Clear
    System Location: Bldg. A412, 2nd Floor, Left cabinet_______     Clear
    System Contact:  Joe Smith 800-555-5555 pager 888-555-5555      Clear



--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu        MainMenu   Exit
 Save
```

Any printable ASCII characters are valid entries for all the Device Name screen inputs. ASCII printable characters include:

- Numeric 0–9
- Upper or lower case A–Z
- Space
- All standard keyboard symbols

Device Name

The Device Name entry appears on all ATI screens. The input on this screen is displayed on the Identity screen. Refer to *Identity Information* on page 3-3.

System Fields

The three System entry fields are alphanumeric and provide 127 characters for each field. The System entries appear on the Identity display as shown in the next section. The SNMP System entry fields are:

- **System Name:** The general SNMP system name.
- **System Location:** The physical location of the SNMP-managed device.
- **System Contact:** Identification information, such as contact name, phone number, or mailing address.

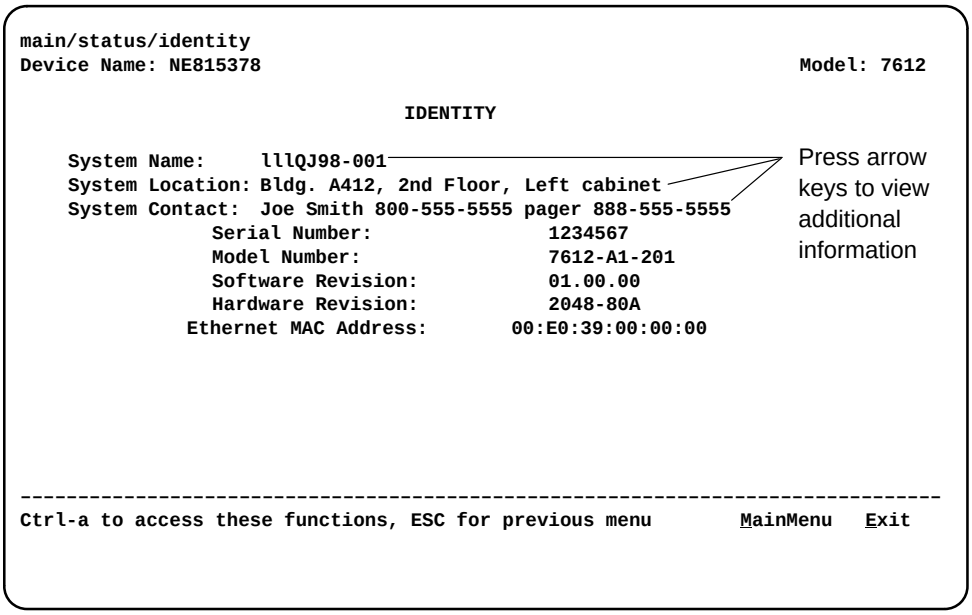
Press Ctrl-a to switch to the screen function key area below the dotted line. Select Save and press Return. When Save is complete, Command Complete appears at the bottom of the screen.

Identity Information

The Identity screen provides identification information about the DSU.

To access the Identity screen, follow this menu selection sequence:

Main Menu → Status → Identity



To view information on the three System entries beyond the 40 characters on the screen, place the cursor on the first or last character and press the left or right arrow.

In addition to the System information entered on the Device Name screen, the Identity screen shows:

- **Serial Number:** The unique serial number of the unit.
- **Model Number:** The model number of the unit.
- **Software Revision:** The revision level of the firmware in the unit.
- **Hardware Revision:** The revision level of circuit card assembly.
- **Ethernet MAC Address:** The Media Access Control address of the Ethernet port, assigned at the time of manufacture.

Configuring the DSU

Configuration option settings determine how the DSU operates. Use the DSU's Configuration branch to display or change configuration option settings.

Configuration Option Areas

The DSU is shipped with factory settings in all configuration option areas. You can find default information by:

- Referring to Appendix A, *Configuration Option Tables*, or Appendix B, *Worksheets*.
- Accessing the Default Factory Configuration branch of the DSU menu.

The DSU offers four sets of configuration option settings located in the following areas. The first three sets match the Default Factory Configuration options set until modified and saved by the user.

If the factory default settings do not support your network's configuration, customize the configuration options for your application.

Configuration Option Area	Configuration Option Set
Current Configuration	The DSU's active set of configuration options.
Customer Configuration 1	Use to set up and store a set for future use.
Customer Configuration 2	Use to set up and store a second set for future use.
Default Factory Configuration	A read-only configuration area containing the factory-default configuration options.

Accessing and Displaying Configuration Options

To display the configuration options, you must first copy one configuration option set into the edit area.

▶ Procedure

To load a configuration option set into the configuration edit area:

1. Follow this menu selection sequence:

   Main Menu → *Configuration* → *Load Configuration From*

2. Select one of the four configuration option areas listed in the table in *Configuration Option Areas* on page 3-4.

3. Press Return. The selected configuration option set is loaded and the Configuration Edit/Display menu screen appears.

No configuration edits are allowed when the effective access level is 2 or 3. Configuration is read-only and allows viewing only of configuration option settings. If the effective access level is not 1:

- The last line of the Load Configuration From screen reads:

  Access Level is *n*, Configuration is read-only

- The Save prompt will not appear on any screens.

Refer to Chapter 4, *Security*.

Saving Configuration Options

When changes are made to the configuration options, the changes must be saved to take effect. The Save key and Save Configuration To screen appear when the user has an effective access level of 1. All other effective access levels have read-only permission.

▶ Procedure

To save configuration options changes:

1. Press Ctrl-a to switch to the screen function key area below the dotted line.
2. Select Save and press Return. The Save Configuration To screen appears.
3. Select one of the three configuration option areas on the screen and press Return. When Save is complete, Command Complete appears in the message area at the bottom of the screen.

NOTE:

If you attempt to leave the edit session without saving your changes, a Save Configuration screen appears requiring a Yes or No response.

If you select . . .	Then the . . .
Yes	Save Configuration To screen appears.
No	Main Menu appears and changes are not saved.

Security

4

Overview

The DSU provides several ways to control access to the ATI through option settings. You can:

- Enable the Login Required option to require a Login ID for the:
  - Terminal Port
  - Telnet Session via the IP interfaces (the 10BaseT port or the IMC)
- Limit the access using:
  - Port Access Level option of 1, 2, or 3 for the Terminal port
  - Session Access Level option of 1, 2 or 3 for the Telnet Session

  Refer to Table 4-1, Effective Access Levels.
- Disable the access using:
  - In-Band Management Channel Rate (bps) option for the IMC
  - Ethernet Port Use option
  - Telnet Session option

Refer to *ATI Access* on page 4-3.

SNMP security is handled through Community Names with access levels and IP address validation. Refer to *Controlling SNMP Access* on page 4-6.

Preventing access to the ATI by setting the In-Band Management Channel Rate or Ethernet Port Use options to Disable also inhibits SNMP management over those interfaces.

Creating a Login

Logins apply to Terminal port access and Telnet access to the ATI. Six login ID/password combinations are available. Each Login ID and Password must be unique and include an access level.

For additional information regarding the ATI access using the Login Required option, refer to *ATI Access* on page 4-3.

▶ Procedure

To create a login record:

1. Follow this menu selection sequence:

   Main Menu → Control → Administer Logins

2. Press Ctrl-a to switch to the screen function key area below the dotted line.
3. Select New and press Return.
4. Create the login by entering the following fields.

On the Administer Logins screen, for the . . .	Enter . . .
Login ID	1 to 10 ASCII printable characters
Password	1 to 10 ASCII printable characters
Access Level	Level 1, Level 2, or Level 3

NOTE:

Assign at least one Level 1 Access Level. Full access is necessary to make configuration option changes and administer logins. If there is no effective Access Level 1, refer to *Device Reset* in Chapter 7, *Testing*.

5. Press Ctrl-a to switch to the screen function key area below the dotted line. Select Save and press Return.
6. When Save is complete, Command Complete appears at the bottom of the screen. Select:

   — New to add another login record

   — MainMenu to go to the Main Menu

   — Exit to end the ATI session

Deleting a Login

▶ Procedure

To delete a login record:

1. Follow this menu selection sequence:

   Main Menu → Control → Administer Logins

2. Press Ctrl-a to switch to the screen function key area below the dotted line.
3. Select PgUp or PgDn and press Return to page through login pages/records until you find the one to be deleted.
4. Once the correct record is displayed, select Delete and press Return.
5. To complete the delete action, select Save and press Return.

   When the deletion is complete, Command Complete appears at the bottom of the screen. The number of login pages/records reflects one less record, and the record following the deleted record appears.

ATI Access

Access to the ATI is available through either the Terminal port or a Telnet session.

Access to the ATI through the Terminal port can be limited. Refer to Table A-5, Terminal Port Options, to:

- Enable Login Required.
- Assign a Port Access Level of 1, 2, or 3.

The ATI can be accessed remotely through a Telnet Session via either the 10BaseT port or the IMC. The DSU provides several methods for limiting access to the ATI through a Telnet session.

- Refer to Table A-6, Telnet Session Options, to:
  - — Enable Login Required.
  - — Assign a Telnet Session Access Level of 1, 2, or 3.
  - — Disable Telnet access completely.
- To prevent the 10BaseT port and IMC from supporting a Telnet session you can also:
  - — Set the Ethernet Port Use option to Disable. Refer to Table A-4, Ethernet Port Options.
  - — Disable the IMC using the In-Band Management Channel Rate (bps) option. Refer to Table A-2, Network Interface Options.

Preventing access to the ATI by setting the In-Band Management Channel Rate or Ethernet Port Use options to Disable also inhibits SNMP management over those interfaces.

Effective Access Level

The ATI effective access level is the more restrictive of:

- Port/Session access level, or
- The Access level associated with the Login ID.

For example, if a login ID is created with an Access Level 1 and the Terminal Port is set for a Port Access Level of 2, the effective access level to the ATI is 2.

Table 4-1. Effective Access Levels

ATI Access to Menu Functions	Effective Access Level 1	Effective Access Level 2	Effective Access Level 3
Status	Full Access	Full Access	Read-Only
Test	Full Access	Full Access	No Access
Configuration	Full Access	Read-Only	Read-Only
Control	Full Access	No Access	No Access

When user access to the ATI is attempted through the Terminal port or a Telnet session, the ATI response is based on the Login Required option and the availability of the ATI.

Table 4-2. ATI Access Conditions

If access to the ATI is through . . .	Then . . .	What to do now?
The Terminal port with – ■ The Login Required option set to Disable (see Table A-5)	The Main Menu screen appears.	Select a menu option to begin your session.
The Terminal port with – ■ The Login Required option set to Enable (see Table A-5)	You are prompted for a login ID and password.	If Invalid Password appears, re-enter the password. After three tries with an invalid password, the user is logged off. Contact the system administrator.
	The Main Menu screen appears if the login ID is not configured yet.	Select a menu option to begin your session.
The Terminal port and the ATI is already in use via Telnet	**User Interface Already In Use** message appears with the active user's IP address and Login ID.	Try again later. When the ATI is available, the message **User Interface Idle** appears.
A Telnet session and the ATI is currently in use via the Terminal port	**Connection Refused** message appears. The DSU allows only one connection at a time.	Try again later.

Controlling SNMP Access

There are three methods for limiting SNMP access.

- Disable the SNMP management option. Refer to Table A-7, General SNMP Management Options.
- Assign SNMP community names and access types. The DSU supports SNMP Version 1, which provides limited security through the use of community names.
- Limit SNMP access through validation of the IP address of each allowed SNMP manager.

Assigning SNMP Community Names and Access Types

The DSU can be managed by an SNMP manager supporting SNMP. The community name must be supplied by an external SNMP manager accessing an object in the MIB.

To define SNMP community names, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → SNMP → General SNMP Management

Refer to Table A-7, General SNMP Management Options, to:

- Enable SNMP Management.
- Assign the SNMP community names of the SNMP Managers that are allowed to access the DSU's Management Information Base (MIB).
- Specify Read or Read/Write access for each SNMP community name.

Limiting SNMP Access through the IP Addresses of the Managers

The DSU provides an additional level of security through validation of the IP addresses.

The SNMP Management option must be enabled. To control SNMP access with IP addresses, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → SNMP → SNMP NMS Security Options

Refer to Table A-8, SNMP NMS Security Options. The SNMP access can be limited by:

- Enabling NMS IP address validation to perform validation checks on the IP address of an SNMP management system attempting to access the DSU.
- Specifying read or read-write access for each NMS authorized to access the unit.

IP Addressing

5

Selecting an IP Addressing Scheme

You can select from many IP (Internet Protocol) addressing schemes to provide SNMP NMS connectivity. Review the following information in preparation for selecting an IP addressing scheme.

- You can assign IP addresses to the:
  - — 10BaseT port
  - — IMC
- When the IMC Routing Information Protocol option is set to Proprietary, IP routing information is automatically passed between interconnected DSUs from the network side.

  A static route to the DSU that is managed over the IMC must be set in the routing table of the NMS host or local router.
- Each DSU's internal routing table supports a maximum of 20 routes, even though a single route is all that is needed to reach every device on a subnet.
- Any legal host address is allowed for a given subnet; the address choice within the subnet is completely arbitrary.
- The 48-bit MAC (Media Access Control) address of the 10BaseT port does not govern the port's 32-bit IP address.

IP Addressing Scheme Examples

Management of IP addressing is based upon individual IP addresses assigned to each interface. The IP interfaces for the unit are the:

- Ethernet port: See Table A-4, Ethernet Port Options.
- IMC: Set the In-Band Management Channel Rate (bps) to 1600, 4000, or 8000 bps; see Table A-2, Network Interface Options.

NOTE:

Do not assign IP addresses without the assistance of the parties who determine the IP addressing scheme used for your organization.

The following illustrations and examples apply to IP management traffic only. The subnet mask for each device in these examples is 255.255.255.000.

IMC Connection – Same Subnet

In this example, the DSU with the IMC IP address of 135.18.2.1 is connected to:

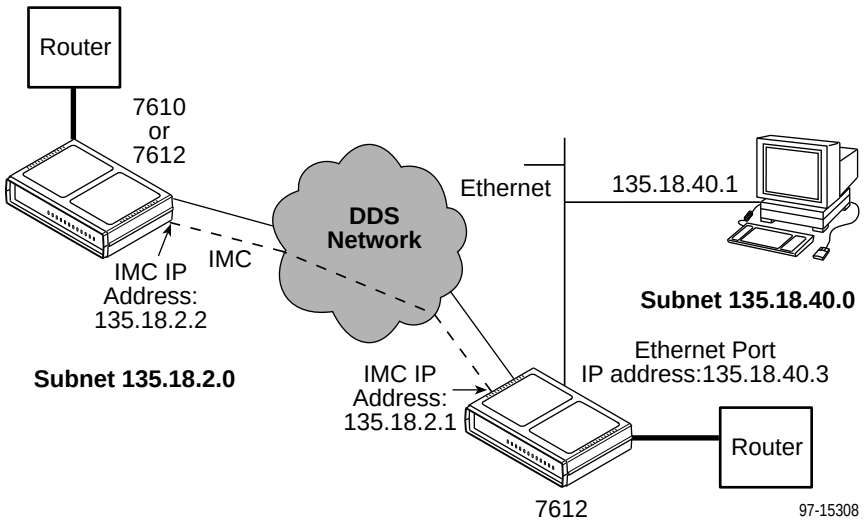
- The NMS at the central site, via the 10BaseT port
- A remote DSU through the proprietary IMC

The IMC is enabled (the rate is set to 1600, 4000, or 8000). See Table A-2, Network Interface Options.

The Default Gateway Address is 000.000.000.000. See Table A-4, Ethernet Port Options.

NOTE:

Interconnected DSUs will automatically pass routing information between each other using a proprietary protocol. However, a static route to subnet 135.18.2.0 must be set in the routing table of the NMS Host.

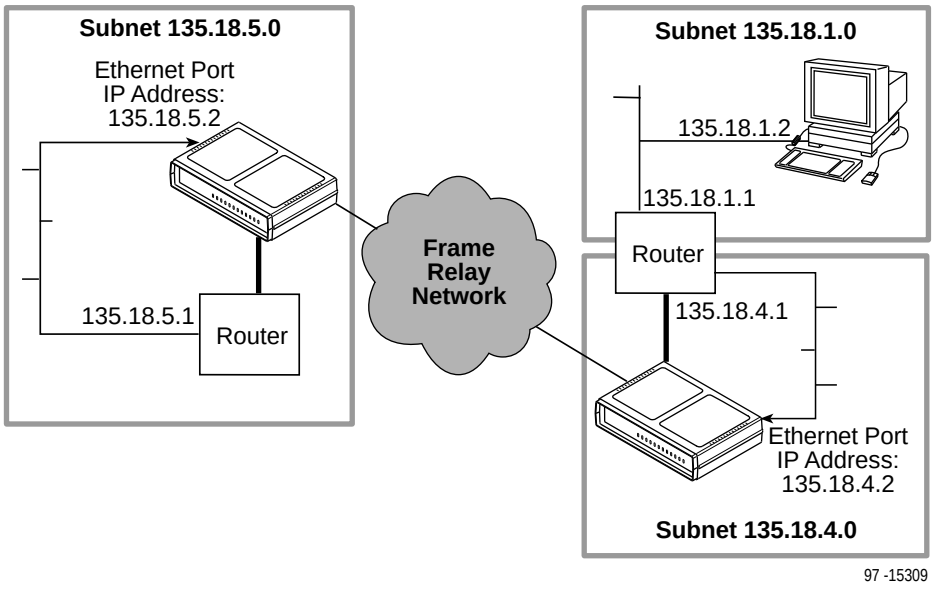


Using Routers to Route DSU Management Data

In this example, the DSUs:

- Receive their management data through the 10BaseT port connection to a hub.
- Do not route the data between themselves. (The IMC is disabled. See Table A-2, Network Interface Options.) Routers route management data for the connected DSUs using the management data path between the routers.

The NMS or Telnet host can be on the same subnet as the DSU, or it can connect to the subnet the DSU is on through a router. If it uses a router, the DSU needs to have a gateway router defined. The Default Gateway Address in the example is 135.18.4.1. See Table A-4, Ethernet Port Options.



Assigning IP Addresses and Subnet Masks

Once you select an IP scheme, assign address(es) to the DSU.

If using the . . .	Then assign the . . .
10BaseT port as a management interface	10BaseT port IP address and subnet mask. Refer to Table A-4, Ethernet Port Options.
IMC	IP address and subnet mask. Refer to Table A-2, Network Interface Options.

The SNMP NMS Security Options screen provides options to perform security checking on the IP address of the SNMP management system attempting to communicate to the DSU. Refer to Table A-8, SNMP NMS Security Options.

Monitoring the DSU

6

What to Monitor

This chapter presents information on how to access and monitor DSU status and performance statistics on the DDS network. You can monitor DSU operations by viewing:

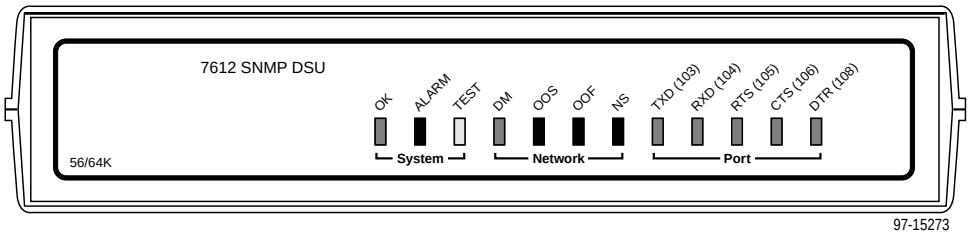
- LEDs on the Display LEDs screen or the DSU's front panel
- System and Test Status screen
- Highest priority Health and Status message on the right on the last line of all screens
- Network Interface Status screen
- Network Performance Statistics screen
- Ethernet Port Statistics screen
- Management Protocol Statistics screen
- SNMP traps and other information reported by your NMS via SNMP MIB objects

  Refer to Appendix C, *MIB Descriptions*, for the SNMP MIBs supported by the DSU.

DSU LEDs

The DSU's 12 LEDs are organized in three groups:

- **System** LEDs display the status of the unit
- **Network** LEDs provide the status of the network interface
- **Port** LEDs display the activity on the user data (DTE) port



The status of the DSU LEDs can be viewed on the Display LEDs screen, both locally and remotely.

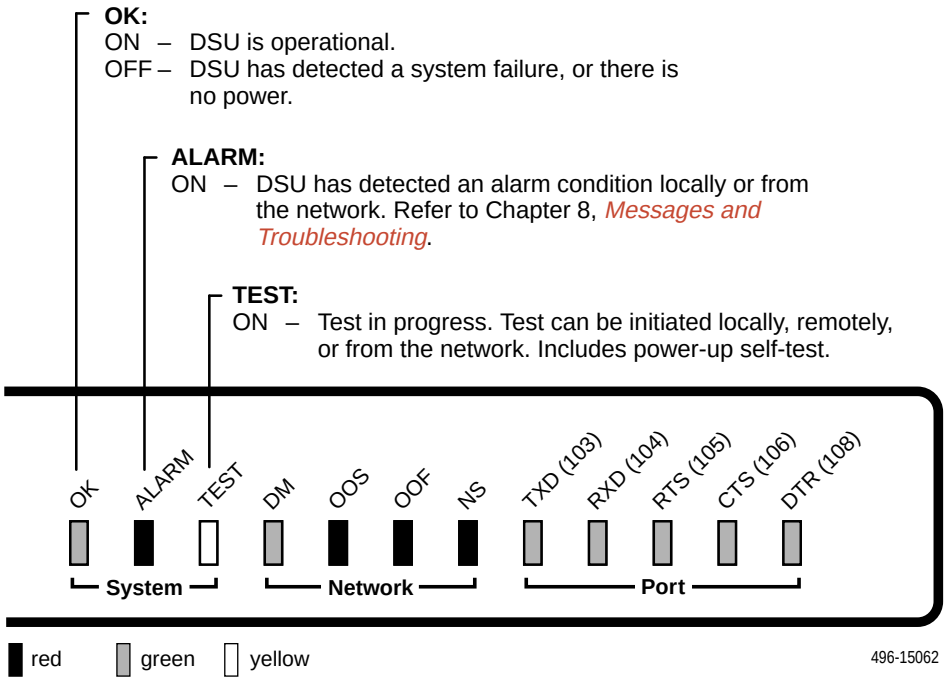
To view the LED status screen, follow this menu selection sequence:

Main Menu → Status → Display LEDs

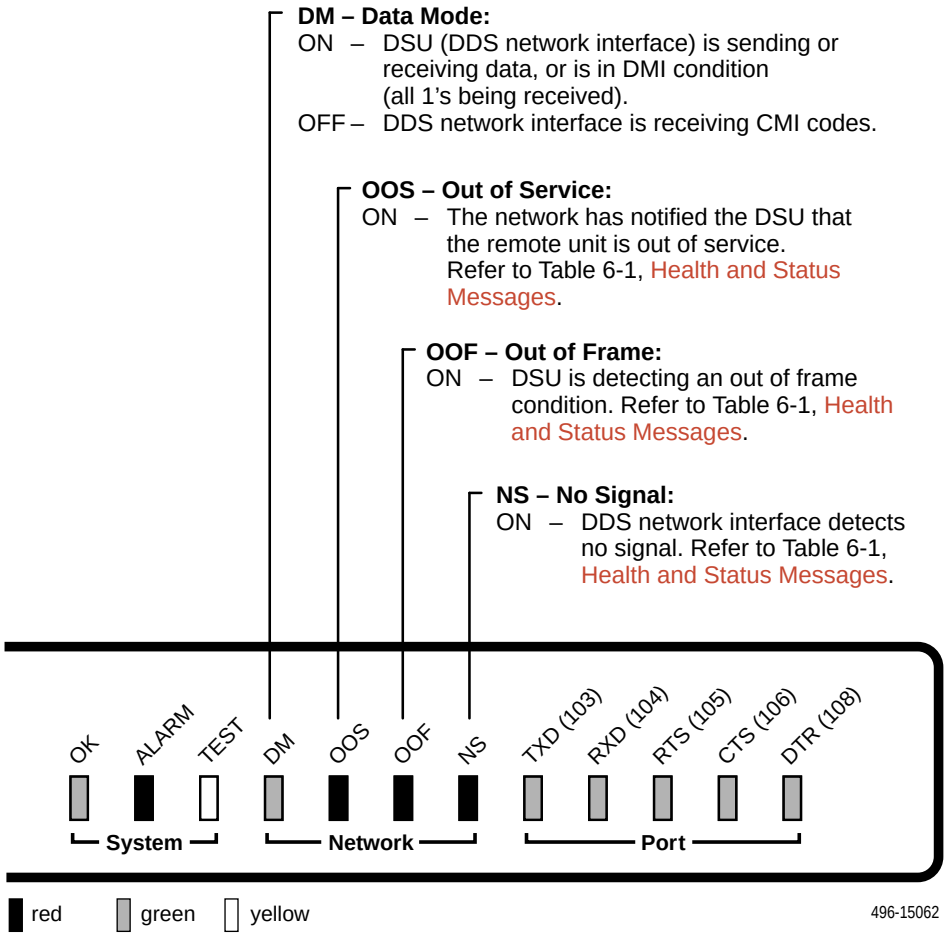
```
main/status/leds
Device Name:                                                    Model: 7612

                              DISPLAY LEDS

        SYSTEM                    NETWORK                         DTE

    OK    ALARM   TEST        DM   OOS   OOF   NS        TXD   RXD  RTS  CTS  DTR


--------------------------------------------------------------------------------
                                ESC for previous menu       MainMenu   Exit
 Refresh
```

When viewed via the ATI, the status display screen is updated approximately every 5 seconds. Use Refresh to obtain a current status of all LEDs.

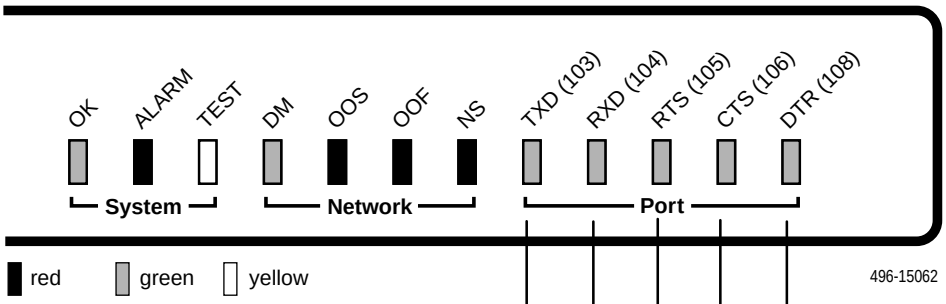
System LEDs


OK:
ON – DSU is operational.
OFF – DSU has detected a system failure, or there is no power.
ALARM:
ON – DSU has detected an alarm condition locally or from the network. Refer to Chapter 8, Messages and Troubleshooting.
TEST:
ON – Test in progress. Test can be initiated locally, remotely, or from the network. Includes power-up self-test.
OK
ALARM
TEST
DM
OOS
OOF
NS
TXD (103)
RXD (104)
RTS (105)
CTS (106)
DTR (108)
System
Network
Port
red
green
yellow
496-15062

Network LEDs



Port LEDs



TXD – Transmitted Data:
ON – Receiving all 0's from the DTE.
OFF – Receiving all 1's from the DTE.
Blinking – User data is being transferred.

RXD – Received Data:
ON – Sending all 1's to the DTE.
OFF – Sending all 0's to the DTE.
Blinking – User data is being transferred.

RTS – Request to Send:
ON – DTE is activating a control signal to indicate readiness to transmit data.

CTS – Clear to Send:
ON – DSU is activating a control signal to indicate to the DTE that it can start sending data.

DTR – Data Terminal Ready:
ON – DTE is activating a control signal to indicate readiness for operation.

Status Screen Commands

The status screens appear with the cursor in the function area below the dotted line. To update the information displayed, select Refresh and press Return.

The System and Test Status screen provides a Clear command. Select Clear and press Return to clear status messages for one-time events.

Statistics screens provide a ClrStats command. Select ClrStats and press Return to clear all statistics and refresh the screen. ClrStats is not available for an Access level of 3.

System and Test Status

Status is a branch of the ATI main menu. From Status, the System and Test Status screen is available and has three sections:

- **Health and Status** – Displays messages in priority order (highest to lowest). Refer to Table 6-1, Health and Status Messages.
- **Self-Test Results** – Results of the Diagnostic test run on the device itself. Refer to Table 6-2, Self-Test Results Messages.
- **Test Status** – Currently active tests. Refer to Table 6-3, Test Status Messages.

To view Health and Status information, follow this menu selection sequence:

Main Menu → Status → System and Test Status

```
main/status/system
Device Name: Node A                                              Model: 7612


                          SYSTEM AND TEST STATUS

HEALTH AND STATUS            SELF-TEST RESULTS   TEST STATUS

Cross Pair Detection         Device Fail         No Test Active
No Signal hhh:mm:ss          Memory Fail         CSU Loopback Active
Out Of Service hhh:mm:ss     Passed              Net-initiated CSU LB Active
Out Of Frame hhh:mm:ss                           DSU Loopback Active
Excessive BPVs hhh:mm:ss                         Net-initiated DSU LB Active
In-Band Fram. Err. hhh:mm:ss                     V.54-initiated DSU LB Active
User Data Port DTR Off                           Local Loopback Active
In-band Mgmt Channel Fail                        Sending 511 on Port
Device Fail yyyyyyyy                             Monitoring 511 on Port
Ethernet Link Down                               Sending 511 on Network
DSU Operational                                  Monitoring 511 on Network
                                                 Lamp Test Active

--------------------------------------------------------------------------------
                                  ESC for previous menu       MainMenu   Exit
Refresh    Clear
```

The following messages appear in the first column of the System and Test Status screen. The messages are listed from high to low priority on the screen but in alphabetical order in Table 6-1. The highest priority Health and Status message also appears on the bottom right of all ATI screens.

Table 6-1. Health and Status Messages (1 of 2)

Message	What Message Indicates	What To Do
Cross Pair Detection	The DDS Receive (RX) and Transmit (TX) pairs are crossed on the network interface. Alarm LED is on.	Reverse the RX and TX pair at the punchdown block or other termination point.
Device Fail *yyyyyyyy*	An internal error has been detected by the operating software. *yyyyyyyy* indicates the 8-digit hexadecimal failure code.	1. Provide the 8-digit failure code shown (*yyyyyyyy*) to your service representative. 2. Use the Clear command to clear the message. 3. Reset the DSU to clear the condition and message.
DSU Operational	The DSU is functioning properly and there are no status messages to display.	No action required.
Ethernet Link Down	The DSU detects no electrical activity on the 10BaseT port.	1. Verify that the Ethernet cable is securely attached at both ends. 2. Contact your LAN support technician if problem persists.
Excessive BPVs *hhh:mm:ss*[1]	Data rates do not match or network trouble causing bipolar violations. Alarm LED is on and Network Performance Statistics are active.	1. Verify that the network cable is securely attached at both ends. 2. Contact network provider if problem persists. 3. Check line rate.
In-Band Fram Err *hhh:mm:ss*[1]	The IMC communication between the local and remote DSU is not working.	1. Verify that the remote unit has IMC set at the same rate. 2. Contact network provider if problem persists.
In-Band Mgmt Channel Fail	The IMC is not operational.	Enable the IMC on the remote unit.
No Signal *hhh:mm:ss*[1]	No signal is being received. Local DSU network problem. The Alarm and NS LEDs are on and Network Performance Statistics are active.	1. Verify that the network cable is securely attached at both ends. 2. Contact network provider.

[1] *hhh:mm:ss* indicates the amount of time the condition has existed in hours, minutes, and seconds. When the maximum time has been exceeded, 255:59:59+ appears.

Table 6-1. Health and Status Messages (2 of 2)

Message	What Message Indicates	What To Do
Out of Frame *hhh:mm:ss*[1]	DSU is detecting an out of frame condition, associated with: ■ Receiving out of frame code from the network. ■ DSU detecting out of frame errors with 64 kbps CC data rate. ■ DSU unable to synchronize local receiver circuit with line signal.	1. Verify that the line rate matches the configured rate. 2. Contact network provider.
Out of Service *hhh:mm:ss*[1]	DSU is receiving out of service code from the network for the remote unit. The Alarm and OOS LEDs are on and Network Performance Statistics are active.	1. Verify that the remote site is in service. 2. Contact network provider.
User Data Port DTR Off	The DTE is not ready to transmit or receive data. This message will not appear unless Monitor DTR is enabled.	1. Check on the DTE status. Verify that the DTE is powered up and asserting DTR. 2. Disable Monitor DTR.
[1] *hhh:mm:ss* indicates the amount of time the condition has existed in hours, minutes, and seconds. When the maximum time has been exceeded, 255:59:59+ appears.		

Self-Test Results

The results of the last power-up or reset self-test appear in the middle column of the System and Test Status screen.

Table 6-2. Self-Test Results Messages

Message	What Message Indicates	What To Do
Device Fail	One or more of the DSU's integrated circuit chips has failed device-level testing.	1. Reset the DSU and try again. 2. Use the Clear command to clear the message. 3. Call your service representative for assistance if the message reappears.
Memory Fail	DSU failed memory verification.	
Passed	The DSU has been plugged in or reset and has passed the diagnostic test. There are no other status messages.	No action required.

Test Status Messages

The Test Status Messages in Table 6-3 appear in the right column of the System and Test Status screen. For additional information on loopbacks, refer to Table 7-1, Loopbacks.

Table 6-3. Test Status Messages

Test Status Message	Meaning
CSU Loopback Active	A CSU Loopback toward the network is currently active. Only applies to a test initiated by the user via the ATI or the NMS.
DSU Loopback Active	A DSU Loopback toward the network is currently active. Only applies to a test initiated by the user via the ATI or the NMS.
Lamp Test Active	The Lamp Test is active, causing the LEDs on the front panel to light.
Local Loopback Active	A local loopback toward the DTE is currently active.
Monitoring 511 on Network	DSU is monitoring a 511 test pattern on the network interface.
Monitoring 511 on Port	DSU is monitoring a 511 test pattern on the DTE port.
Net-initiated CSU LB Active	A CSU Loopback initiated by the network is currently active. ■ If the network service is 56 kbps, the network loopback is non-latching. A non-latching loopback ends when the network activation codes stop. ■ If the network service is 64 kbps CC, the network loopback is latching.
Net-initiated DSU LB Active	A DSU Loopback initiated by the network is currently active. ■ If the network service is 56 kbps, the network loopback is non-latching. A non-latching loopback ends when the network activation codes stop. ■ If the network service is 64 kbps CC, the network loopback is latching. This condition can only occur when the Network Interface option Network-initiated DSU Loopback (64K CC) is enabled. Refer to Table A-2, Network Interface Options.
No Test Active	Status message, indicating no local, remote, or network test in progress.
Sending 511 on Network	A 511 test pattern is being sent over the network interface.
Sending 511 on Port	A 511 test pattern is being sent over the DTE port.
V.54-initiated DSU LB Active	A DSU loopback is active that was initiated by the detection of a V.54 sequence originated by the remote unit. This condition can only occur when V.54 Initiated DSU Loopback is enabled. Refer to Table A-2, Network Interface Options.

Network Interface Status

To view the Network Interface Status, follow this menu selection sequence:

Main Menu → Status → Network Interface Status

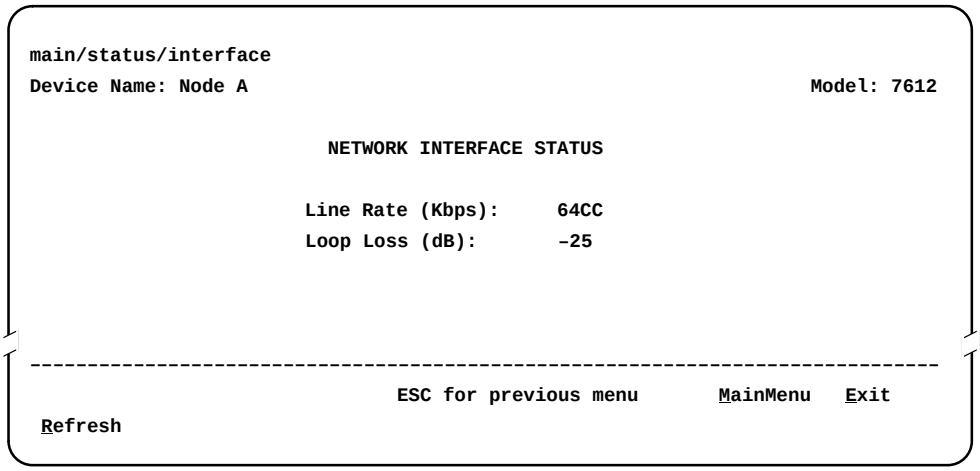


Table 6-4 describes the fields on the Network Interface Status screen.

Table 6-4. Network Interface Status Screen Contents

Field	Status	What the Status Indicates
Line Rate (Kbps)	56 64CC 64LADS Autobaud	Line rate on the network interface. Autobaud indicates the DSU is trying to determine the network line rate. If this does not change to a numeric value within about 25 seconds, you may need to set the Line Rate manually.
	No Signal	No signal can be detected over the network interface.
Loop Loss (dB)	0 to –65	Amount of loop loss – loss of signal strength of the receive line signal from the local loop, measured in decibels.
	Inoperative	The line may be disconnected.

Network Performance Statistics

To view the Network Performance Statistics, follow this menu selection sequence:

Main Menu → Status → Network Performance Statistics

```
main/status/performance
Device Name:                                                    Model: 7612


                    NETWORK PERFORMANCE STATISTICS

                No Signal Count:        101920     26:33:08
                Out of Service Count:        0      0:00:00
                Out of Frame Count:        621      8:53:49
                Excessive BPV Count:     99830    144:28:11
                Invalid BPV Count:       87409


--------------------------------------------------------------------------------
                                ESC for previous menu        MainMenu   Exit
 Refresh    ClrStats
```

Table 6-5 describes the fields on the Network Performance Statistics screen.

Table 6-5. Network Performance Statistics Screen Contents

Label	What the Field Indicates
No Signal Count	The number of occurrences of a No Signal condition.
Out of Service Count	The number of occurrences of an Out of Service condition.
Out of Frame Count	The number of occurrences of an Out of Frame condition.
Excessive BPV Count	The number of occurrences of an Excessive Bipolar Violation (BPV) condition. This is defined as at least one Invalid BPV every 20 ms for a 2-second period.
Invalid BPV Count	The total number of Invalid BPVs detected.

All counts show the number of occurrences since the last reset of the counters. In the last column, *hhh:mm:ss* indicates the amount of time the condition has existed in hours, minutes, and seconds. When the maximum time has been exceeded, 255:59:59+ appears.

Ethernet Port Status

To view the Ethernet (10BaseT) Port Status, follow this menu selection sequence:

Main Menu → Status → Ethernet Port Status

```
main/status/ethernet
Device Name: Node A                                              Model: 7612

                          ETHERNET PORT STATUS

                 Port Use:                802.3
                IP Address:               000.000.000.000
                Subnet Mask:              000.000.000.000
                Default Gateway Address:  000.000.000.000
                Ethernet MAC Address:     00:E0:39:00:00:00

                Frames Transmitted:       0000000000
                Frames Received:          0000000000
                Errored Frames:           0000000000
                Excessive Collisions:     0000000000
                Carrier Sense Errors:     0000000000
                Deferred Transmissions:   0000000000

--------------------------------------------------------------------------------
                            ESC for previous menu       MainMenu   Exit
 Refresh        ClrStats
```

Table 6-6 describes the fields on the Ethernet Port Status screen.

Table 6-6. Ethernet Port Status Screen Contents (1 of 2)

Label	What the Field Indicates
Port Use	The port is enabled if 802.3 or Version 2 is displayed.
IP Address	The IP address of the port.
Subnet Mask	The subnet mask to be used with the IP address.
Default Gateway Address	The gateway to be used for packets that do not have a route.
Ethernet MAC Address	The physical address of the port.
Frames Transmitted	The number of frames transmitted.
Frames Received	The number of frames received.
Errored Frames	The number of frames in error. This is the sum of frames with alignment errors, FCS (Frame Check Sequence) errors, and framing errors.
Excessive Collisions	The number of frames for which transmission failed due to excessive collisions.

Table 6-6. Ethernet Port Status Screen Contents (2 of 2)

Label	What the Field Indicates
Carrier Sense Errors	The number of times the carrier sense condition was lost or never asserted.
Deferred Transmissions	The number of frames for which the first transmission attempt is delayed because the medium is busy.

All counts show the number of occurrences since the last reset of the counters.

Management Protocol Statistics

To view the Management Protocol Statistics, follow this menu selection sequence:

Main Menu → Status → Management Protocol Statistics

```
main/status/management
Device Name: Node A                                              Model: 7612

                          MANAGEMENT PROTOCOL STATISTICS

                                      IP          TCP          UDP

         Datagrams Transmitted:        0            0            0
         Datagrams Received:           0            0            0
         Format Errors:                0            0            0
         Invalid Address:              0            –            0
         Unknown Protocol:             0            –            –
         Dropped Due To No Route:      0            –




--------------------------------------------------------------------------------
                             ESC for previous menu       MainMenu   Exit
 Refresh         ClrStats
```

Table 6-7 describes the fields on the Management Protocol Statistics screen.

Table 6-7. Management Protocol Statistics Screen Contents

Label	What the Field Indicates
Datagrams Transmitted	The number of datagrams successfully transmitted at each protocol layer.
Datagrams Received	The number of datagrams successfully received at each protocol layer.
Format Errors	The number of protocol packets that contained errors.
Invalid Address	The number of protocol packets that contained invalid addresses.
Unknown Protocol	The number of datagrams that were lost due to unknown protocols.
Dropped Due to No Route	The number of datagrams that were lost due to no route.

All counts show the number of occurrences since the last reset of the counters.

Testing

7

Detecting Problems

The DSU can detect and report problem conditions and perform diagnostic tests. The DSU offers a number of indicators to alert you to possible problems:

- LEDs – Refer to *DSU LEDs* in Chapter 6, *Monitoring the DSU*.
- SNMP Traps – For information on traps, refer to *Configuring SNMP Traps* in Chapter 8, *Messages and Troubleshooting*.
- Health and status messages and network performance statistics. Refer to Chapter 6, *Monitoring the DSU*.
- Alarm Condition Indications.

The following table shows the available indicators of alarm conditions on the network interface and the User Data port.

Alarm Condition	SNMP Trap	ATI Status Screen	Alarm LED	Specific LED
Crossed Pairs	Y[1]	Y	Y	N
No Signal (NS)	Y[1]	Y	Y	Y
Out of Service (OOS)	Y[1]	Y	Y	Y
Out of Frame (OOF)	Y[1]	Y	Y	Y
Excessive Bipolar Violations (BPV)	Y[1]	Y	Y	N
Inband Framing Error	N	Y	Y	N
DTR Off	Y[1]	Y	N	Y
[1] Link Up/Link Down Trap				

Tests Available

From the Test menu, you can run network tests, data port tests, and a lamp test for the front panel LEDs. Loopbacks can be initiated locally and remotely. Refer to Table 7-1, Loopbacks.

The Test menu is limited to users with an access level of 1 or 2. To access the Test menu, follow this menu selection sequence:

Main Menu → Test

```
main/test
Device Name: Node A                                          Model: 7612


                                    TEST

                               Network Tests
                               Data Port Tests
                               Lamp Test


                               Abort All Tests


--------------------------------------------------------------------------------
                                ESC for previous menu       MainMenu   Exit
```

Network-initiated tests require the participation of your network service provider.

The DSU supports physical-level tests independently on a per-interface basis.

- The CSU and DSU loopbacks and 511 test pattern send/monitor are supported on the network interface.
- The Local Loopback and 511 test pattern send/monitor are supported on the DTE port.

Network Tests

To access the Network Tests screen, follow this menu selection sequence:

Main Menu → Test → Network Tests

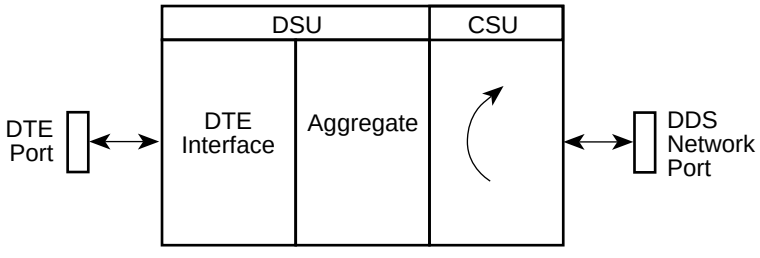
```
main/test/network
Device Name:                                                    Model: 7612

                              NETWORK TESTS

    Test            Command   Status          Result

    CSU Loopback:   Start     Inactive          0:00:00
    DSU Loopback:   Start     Inactive          0:00:00

    Send V.54 Up:   Send      Inactive
    Send V.54 Down: Send      Inactive

    Send 511:       Start     Inactive          0:00:00
    Monitor 511:    Stop      Active          125:08:48    Errors 99999+




--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu   Exit
 ResetMon
```

Use the Command column to start or stop a test by pressing Enter. The Result column displays the test duration since the last device reset. When the Monitor 511 test is active, ResetMon is available to reset the error counter to zero.

A network-initiated loopback is not affected by the Test Timeout option, the Stop command on the Network Test screen, or the Abort All Tests command from the Test menu.

CSU or External Network Loopback

CSU loopback is an external loopback that is located as closely as possible to the network interface. An active CSU loopback disrupts IP data going over the IMC.

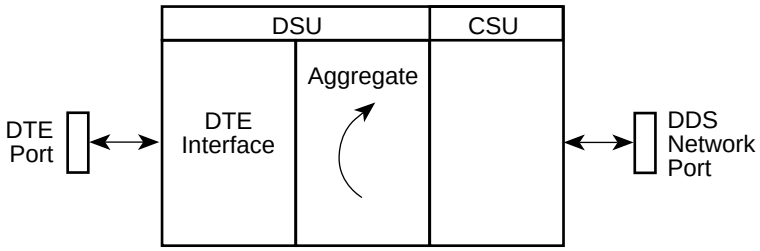


CSU Loopback 496-15144

DSU or Internal Network Loopback

DSU loopback is an internal loopback that is located as closely as possible to the customer interface serving the DTE.

An active DSU loopback initiated from the network disrupts IP data going over the IMC. However, this test is not disruptive when initiated by the user (via ATI) or by the NMS.



DSU Loopback 496-15160

Send V.54 Up/Down Sequences

The local DSU can send an ITU-T V.54 Up or Down sequence to request the activation or termination of a DSU (digital) loopback of a remote unit. This is the same as the DSU Loopback shown above except the test is activated remotely.

The DSU can send:

- In-band V.54 Up (activation) code to request a Remote DSU Loopback (V.54 Loop 2) at the remote DSU, or
- In-band V.54 Down (deactivation) code to request the termination of a Remote DSU Loopback (V.54 Loop 2) at the remote DSU.

To initiate a send sequence, select the appropriate Send command. Sending appears in the Status column followed (after 3 seconds) by Command Complete at the bottom of the screen.

511 Test Pattern for the Network

This test sends and/or monitors the 511 test pattern over the network interface.

The Monitor 511 test also provides an error counter that can be reset.

To start sending and/or monitoring, select the appropriate Start command.

Data Port Tests

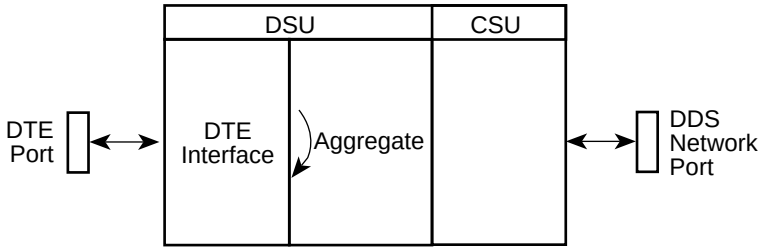
To access the Data Port Tests screen, follow this menu selection sequence:

Main Menu → Test → Data Port Tests

```
main/test/port
Device Name: Node A                                                Model: 7612


                              DATA PORT TESTS

        Test                  Command    Status        Result

        Local Loopback:       Start       Inactive     000:00:00

        Send 511:             Start       Inactive     000:00:00
        Monitor 511:          Stop        Active       255:59:59+ - Errors 99999+


--------------------------------------------------------------------------------
                                   ESC for previous menu       MainMenu   Exit
 ResetMon
```

Local Loopback

Local Loopback loops the user data back to the DTE. This loopback is located as closely as possible to the User Data Port (DTE) interface.



Local Loopback 97-15344

511 Test Pattern for the DTE

This test sends and monitors a 511 test pattern over the User Data Port interface.

The 511 monitor expects the external equipment to provide the clock for the 511 pattern on the interchange circuit CT113 – Transmit Signal Element Timing – DTE Source (XTXC or TT) for timing the incoming pattern. Refer to *DTE Port (V.35) Connector* in Appendix E, *Cables and Pin Assignments*.

Lamp Test

The DSU supports a Lamp test from the Test menu to determine whether all LEDs are lighting and functioning properly.

During the Lamp test, all LEDs blink simultaneously every second. When you stop the Lamp test, the LEDs are restored to their normal condition.

Ending an Active Test

A test initiated by the user can be ended by the user.

- A Test Timeout option is available to automatically terminate a user-initiated Loopback or Pattern test (as opposed to manually terminating a test) after it has been running a specified period of time. Refer to Table A-1, System Options.

  Test Timeout does not pertain to tests commanded by the:

  — Network, such as the network-initiated CSU and DSU Loopbacks.

  — DTE, such as the DTE-initiated Local Loopback.

- On each test screen is a command column. Pressing Return when the cursor is on the Stop command stops the test.

- Use the Abort All Tests selection from the Test menu to stop all tests running on all interfaces, with the exception of network or DTE-initiated loopbacks. Command Complete appears when all tests on all interfaces have been terminated.

Test status messages appear in the right column of the System and Test Status screen. See Table 6-3, Test Status Messages, in Chapter 6, *Monitoring the DSU*.

Loopbacks

Loopbacks can be started from a variety of points in the network. Refer to Table 7-1 for further information.

Table 7-1. Loopbacks

Loopback Type	Initiated By	Notes
Bilateral Loopback	■ ATI ■ NMS ■ Remote unit sending V.54 sequence	When enabled, running a DSU loopback also automatically starts a local loopback. Refer to Table A-3, Data Port Options, to enable.
56 kbps CSU Loopback (Non-latching loopback) 64 kbps CC CSU Loopback (Latching loopback)	■ ATI (Network tests) ■ NMS ■ DDS Network, by loop current reversal	When initiated by the network, CSU Loopback cannot be disabled by the user. When IMC is enabled, the aggregate data is looped back to the network.
DSU Loopback (Digital)	■ ATI ■ NMS	When IMC is enabled, only user data is looped back to the network. Refer to Table A-3, Data Port Options.
Local Loopback	■ ATI ■ DTE via CT141 ■ NMS	Control via CT141 can be disabled. Refer to Table A-3, Data Port Options.
Network-initiated 56 kbps DSU Loopback (Non-latching loopback)	■ DDS Network	When IMC is enabled, the aggregate data stream is looped back to the network. Cannot be disabled by user.
Network-initiated 64 kbps CC DSU Loopback (Latching loopback)	■ DDS Network	Includes optional data scrambling and uses 25-second timer to detect the network sequence. When IMC is enabled, the aggregate data stream is looped back to the network. Can be disabled by user.
Remote Digital Loopback	■ Remote unit sending V.54 sequence	Same as a DSU Loopback but initiated by a remote unit via V.54 sequence. When IMC is enabled, only user data is looped back to the network. Can be disabled locally. Refer to Table A-2, Network Interface Options.
V.54 Sequences to remote unit	■ ATI ■ NMS ■ DTE via CT140	Control via CT140 can be disabled. Refer to Table A-3, Data Port Options.

Device Reset

The DSU can be reset locally or remotely. From the Control menu, select Reset Device and press Return, then answer Yes to the verification message. The DSU reinitializes itself, performing a Device Self-Test. Refer to Table 6-2, Self-Test Results Messages, in Chapter 6.

Configuring the DSU improperly could make the user interface inaccessible, leaving it in a state where an ATI session cannot be started through the Terminal port or via a Telnet session. If this occurs, DSU connectivity can be restored with a terminal that is directly connected and set for Terminal Port option defaults.

Two methods can be used to restore access to the ATI. Both methods cause a device reset.

- **Reset Terminal Port** – Allows you to only reset the configuration options related to Terminal port usage. No security-related configuration options are changed. Refer to Table A-5, Terminal Port Options, for defaults.
- **Reload Factory Defaults** – Allows you to reload the Default Factory Configuration, resetting all of the configuration areas and control settings for security reasons. This method is useful when the user's passwords have been forgotten.

▶ Procedure

To reset Terminal port settings:

1. At the asynchronous terminal connected to the Terminal port, verify that the terminal's options are set to the default settings:
   - — Data Rate(Kbps) to 9.6
   - — Character Length to 8
   - — Stop Bits to 1
   - — Parity to None
2. Power the DSU Off and back On. The DSU performs a power-up routine.
3. Immediately after the OK and TEST LEDs light up, press the Return key 5 times quickly in succession. The System Paused screen appears.

4. Tab to the desired option, and enter yes (or y) for the selected prompt.

If entering yes to prompt . . .	Then all . . .
Reset Terminal Port Options	Terminal port options are set to their factory default values. Refer to Table A-5, Terminal Port Options.
Reload Factory Defaults	Factory default settings contained in the Default Factory Configuration area are loaded in Current, Customer 1, and Customer 2 configuration areas. Any changes to configuration and control settings will be replaced by the factory defaults.

If no (or n) is entered, or if no selection is made within 30 seconds, the DSU returns to the condition or operation it was in when the system pause was initiated, with the Terminal port data rate returning to its configured rate.

5. If yes (or y) is entered, the DSU resets itself and initiates a Device Self-Test. Connectivity is restored and the User Interface Idle screen appears.

Messages and Troubleshooting

8

Overview

There are many messages available to help you assess the status of the device and contribute to problem resolutions. Refer to the following sections:

- *Configuring SNMP Traps*
- *Device Messages*
- *Troubleshooting*

Configuring SNMP Traps

An SNMP trap can be automatically sent out through the IMC or the 10BaseT port to the SNMP manager when the DSU detects conditions set by the user. These traps enable the SNMP manager to gauge the state of the network. Refer to Appendix D, *Standards Compliance for SNMP Traps*, for details of SNMP traps supported by the DSU.

To configure the DSU for SNMP traps, use the SNMP Traps Options screen to:

- Enable SNMP traps.
- Set the number of SNMP managers that receive SNMP traps from the DSU.
- Enter an IP address and network destination for each SNMP manager specified.
- Select the type of SNMP traps to be sent from the DSU.

To configure SNMP Traps, follow this menu selection sequence:

Main Menu → *Configuration* → *Load Configuration From* → *Edit* → *SNMP* → *SNMP Traps*

Refer to Table A-9, SNMP Traps Options.

Device Messages

The Device Messages in Table 8-1, listed in alphabetical order, may appear in the messages area at the bottom of the ATI screens.

Table 8-1. Device Messages (1 of 2)

Device Message	What Message Indicates	What To Do
Blank Entries Removed	New had been selected from the Administer Logins screen, no entry was made, and Save was selected.	■ No action needed. ■ Reenter the Login ID, Password, and Access Level.
Cannot Save – No Login IDs with Access Level 1	An attempt was made to save logins with Access Levels 2 and 3 only.	Create a Login with Access Level 1.
Command Complete	Action requested has successfully completed.	No action needed.
Invalid Character (*x*)[1]	An invalid ASCII character has been entered.	Reenter information using valid characters.
Invalid – Network Initiated CSU (or DSU) Loopback Active	Network-initiated loopback was in progress when another selection was made.	No action needed.
Invalid Password	Login is required and an incorrect password was entered; access is denied.	■ Try again. ■ Contact your system administrator to verify your password.
Invalid – [Test] Already Active	[Test] can be a CSU, DSU, or DTE Local Loopback, or a Send 511 or Monitor 511. The [test] was already in progress when another selection was made.	■ Allow test to continue. ■ Select another test. ■ Stop the test.
Invalid Test Combination	A loopback or 511 pattern test was in progress when Start was selected to start another test, or was active on the same or another interface when Start was selected.	■ Wait until other test ends and message clears. ■ Abort all tests from the Test menu screen. ■ Stop the test from the same screen the test was started from.
Limit of six Login IDs reached	An attempt to enter a new login ID was made, and the limit of six login/password combinations has been reached.	1. Delete another login/password combination. 2. Reenter the new login ID.

[1] *x* is the character not being accepted.

Table 8-1. Device Messages (2 of 2)

Device Message	What Message Indicates	What To Do
No Security Records to Delete	Delete was selected from the Administer Login screen, and no security records had been defined.	■ No action needed. ■ Enter a security record.
Password Matching Error – Re-enter Password	Password entered in the Re-enter Password field of the Administer Logins screen does not match what was entered in the Password field.	■ Try again. ■ Contact your system administrator to verify your password.
Please Wait	Command takes longer than 5 seconds.	Wait until message clears.
Test Active	A test is running and no higher priority health and status messages exist.	■ Contact service provider if test was initiated by the network. ■ Wait until the other test ends and message clears. ■ Cancel all tests from the Test screen. ■ Stop the test from the same screen the test was started from.

Troubleshooting

This DSU is designed to provide you with many years of trouble-free service. If a problem occurs, however, refer to Table 8-2 for possible solutions.

Table 8-2. Troubleshooting (1 of 2)

Symptom	Possible Cause	Solutions
Alarm LED is on.	One of several alarm conditions exists. Health and Status displays the alarm condition.	Refer to Table 6-1, Health and Status Messages, for recommended action.
Cannot access the DSU via the ATI.	Login or password is incorrect, Terminal port is misconfigured, or the DSU otherwise configured so it prevents access.	■ Power the DSU off and on and try again. ■ If problem recurs, try to access the ATI through a Telnet session. ■ Reload Factory Defaults. Refer to *Device Reset* in Chapter 7. ■ Do a Device Reset. Refer to *Device Reset* in Chapter 7.

Table 8-2. Troubleshooting (2 of 2)

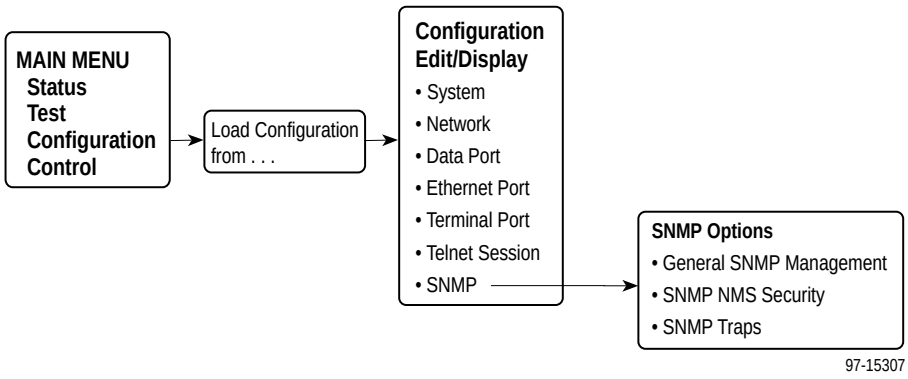
Symptom	Possible Cause	Solutions
Device Fail appears on the System and Test Status screen under Self-Test results.	The DSU detects an internal hardware failure.	■ Power the DSU off and on and try again. ■ Clear the message using the Clear command. ■ Contact your service representative.
An LED is not lit.	LED is burned out.	Run the Lamp test. If the LED in question does not flash with the other LEDs, then contact your service representative.
No power, or the LEDs are not lit.	The power cord is not securely plugged into the wall receptacle and into the rear panel connection.	Check that the power cord is securely attached at both ends.
	The wall receptacle has no power.	■ Check the wall receptacle power by plugging in some equipment that is known to be working. ■ Check the circuit breaker. ■ Verify that your site is not on an energy management program.
Not receiving data; DSU is not responding.	■ DDS line rate/speed has changed. ■ Excessive BPVs causing DSU to become stuck in Autobaud mode. ■ Excessive Loop Loss causing DSU to become stuck in Autobaud mode.	■ Verify that your subscriber loop is running at 56 or 64 CC kbps. ■ Verify that the DSU is set to the same rate as your subscriber loop. (The DSU's rate is displayed on the Network Interface Status screen.) ■ If getting Excessive BPVs, verify that you do not have a bad cable. If the cable is good, contact the network provider. ■ If getting excessive Loop Loss (dB) indications, install a higher quality cable. For maximum distances in LADS applications, refer to Table F-3 in Appendix F. ■ If the DDS Line Rate (Kbps) field shows Autobaud, the DSU may be stuck in Autobaud mode. Configure Line Rate (Kbps) for 56 or 64 kbps. ■ Run Loopback tests. Refer to *Tests Available* in Chapter 7.
Power-Up Self-Test fails. Only Alarm LED is on after power-up.	The DSU has detected an internal hardware failure.	■ Reset the DSU and try again. ■ Contact your service representative.

Configuration Option Tables

A

Overview

The tables in this appendix summarize the configuration options accessed when you select Configuration on the Main Menu. The configuration options are arranged into groups based upon functionality.



Select . . .	To Access the . . .	To Configure the . . .
System	System Options, Table A-1	General system options.
Network	Network Interface Options, Table A-2	DDS network interface.
Data Port	Data Port Options, Table A-3	DTE port.
Ethernet Port	Ethernet Port Options, Table A-4	10BaseT port.
Terminal Port	Terminal Port Options, Table A-5	Terminal port.
Telnet Session	Telnet Session Options, Table A-6	Telnet user interface.
SNMP	■ General SNMP Management Options, Table A-7 ■ SNMP NMS Security Options, Table A-8 ■ SNMP Traps Options, Table A-9	Management support through SNMP.

All changes to configuration options must be saved. Refer to *Saving Configuration Options* in Chapter 3, *Configuring the DSU*.

System Options Menu

For System Options, refer to Table A-1. To access the System Options screen, follow this menu selection sequence:

Main Menu → *Configuration* → *Load Configuration From* → *Edit* → *System*

Table A-1. System Options (1 of 3)

Operating Mode
Possible Settings: **DDS**, **LADS** Default Setting: **DDS**
The unit's operating mode depends upon the DSU's application. **DDS** – Standard DDS network operation. The operating rate is either 56 kbps or 64 kbps CC. **LADS** – The Local Area Data Set operating mode requires that the local and remote units are connected directly to each other. This is a point-to-point application; also known as LDM.

Table A-1. System Options (2 of 3)

DDS Line Rate (Kbps)
Possible Settings: **56, 64CC**, **Autobaud** Default Setting: **Autobaud**
The unit starts up with Autobaud. On the Network Interface Status screen, when the DDS line rate obtained from the service provider is detected, Autobaud is replaced with the actual rate. ■ DDS Line Rate (Kbps) option appears when Operating Mode is set to DDS. NOTES: – Setting the actual data rate will result in minimum power-up time. (If both DSUs use Autobaud, training can take several minutes.) Configuring the actual data rate is recommended after initial installation. – The clock rates generated by the DSU at the DTE interface (TXC and RXC) equal the operating rate minus the configured rate of 1600, 4000, or 8000 bps for the IMC, if enabled. Refer to the In-Band Management Channel Rate (bps) option in Table A-2. **56** – 56 kbps line rate. **64CC** – 64 kbps Clear Channel on a 72 kbps circuit. **Autobaud** – This setting is automatically changed to the actual operating line rate of 56 kbps or 64CC as soon as the signal is detected.
LADS Timing
Possible Settings: **Internal, External, Receive** Default Setting: **Internal**
Determines the timing source for the unit. ■ LADS Timing option appears when Operating Mode is set to LADS. **Internal** – Timing derived from the unit's local clock. Use this setting for the LADS primary timing unit that establishes the timing for both point-to-point units. **External** – Timing is derived from the external clock provided by the DTE connected to the V.35 interface on circuit CT113 (pins U, W). NOTE: The valid rate generated by the DTE must be equal to the LADS line rate minus the configured rate of 1600, 4000, or 8000 bps for the IMC, if enabled. Refer to the In-Band Management Channel Rate (bps) option in Table A-2. **Receive** – Timing is derived from the line receive signal unless the unit is running diagnostic tests. During the tests, the timing source is the internal clock. This setting should be used for a LADS secondary timing unit.
LADS Line Rate (Kbps)
Possible Settings: **56, 64** Default Setting: **64**
Line operating rate for LADS operation. ■ LADS Line Rate (Kbps) option appears when Operating Mode is set to LADS. **56** – 56 kbps line rate. Provides increased distance for the LADS applications. **64** – 64 kbps line rate.

Table A-1. System Options (3 of 3)

Test Timeout
Possible Settings: **Enable**, **Disable** Default Setting: **Enable**
Allows user-initiated tests to end automatically. Recommend enabling when the unit is managed remotely through the IMC to avoid the requirement to terminate the test manually. **Enable** – User-initiated loopback and pattern tests end when test duration is reached. **Disable** – Tests can be terminated manually from the Network Tests screen. Refer to *Network Tests* in Chapter 7. NOTE: Tests initiated by the DTE or network are not affected by this test timeout.
Test Duration (min)
Possible Settings: **1–120** Default Setting: **10**
Number of minutes for a test to be active before automatically ending. ■ Test Duration (min) option appears when Test Timeout is enabled. **1 to 120** – Amount of time in minutes for a user-initiated test to run before terminating.

Network Interface Options Menu

For Network Interface Options, refer to Table A-2. To access the Network Interface Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → Network

Table A-2. Network Interface Options (1 of 2)

Network-initiated DSU Loopback (64K CC)
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Indicates whether the access unit responds to a latching DSU loopback sequence sent by the network as specified by TR62310. ■ Network-initiated DSU Loopback (64K CC) option appears when Operating Mode is set to DDS in Table A-1. **Enable** – Responds to network-initiated commands to start and stop a latching DSU loopback. **Disable** – DSU will not respond to a latching DSU loopback initiated by the network.
Data Scrambling (64K CC)
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Data scrambling is used to suppress the possible simulation of network-initiated DSU latching loopback commands by application data. NOTE: The local and remote units must be set the same. ■ Data Scrambling (64K CC) option appears when Operating Mode is set to DDS in Table A-1. **Enable** – Enables data scrambling. **Disable** – No data scrambling.
V.54 Initiated DSU Loopback
Possible Settings: **Enable, Disable** Default Setting: **Disable**
When enabled, user data is looped back to the network when a V.54 Loop Up sequence is received. The DSU loopback ends when a V.54 Loop Down sequence is detected. **Enable** – DSU loopback can be initiated or terminated by a remote unit sending in-band V.54 Loop 2 Up or Down sequences. **Disable** – V.54 Loop 2 sequences are ignored.
In-Band Management Channel Rate (bps)
Possible Settings: **Disable, 1600, 4000, 8000** Default Setting: **Disable**
The IMC provides a non-disruptive management channel to the remote DSU and uses a portion of the DTE line rate. **Disable** – The IMC is inactive. **1600, 4000, or 8000** – Sets the amount of the line rate in bps to allocate to the IMC. NOTE: The local and remote units must be set the same.

Table A-2. Network Interface Options (2 of 2)

IMC IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the Internet Protocol address used to access the unit via the IMC interface. ■ IMC IP Address option does not appear when the In-Band Management Channel Rate (bps) is disabled. **000.000.000.000 – 223.255.255.255** – The range for the first byte is 000 to 223, with the exception of 127. The range for the remaining three bytes is 000 to 255. **Clear** – Clears the IMC IP address and sets to all zeros.
IMC Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask used to access the unit via the IMC interface. ■ IMC Subnet Mask option does not appear when the In-Band Management Channel Rate (bps) is disabled. **000.000.000.000 – 255.255.255.255** – Set the IMC interface subnet mask. The range for each byte is 000 to 255. **Clear** – Clears the IMC Subnet Mask and sets to all zeros. When the subnet mask is all zeros, the device creates a default subnet mask based on the class of IP address: – Class A defaults to 255.000.000.000 – Class B defaults to 255.255.000.000 – Class C defaults to 255.255.255.000
IMC Routing Information Protocol
Possible Settings: **None, Proprietary** Default Setting: **Proprietary**
The RIP routes IMC management information between devices. ■ IMC Routing Information Protocol does not appear when the In-Band Management Channel Rate (bps) option is disabled. **None** – No routing protocol. **Proprietary** – Uses proprietary variant of RIP Version 1 to enable the routing of IP traffic between Paradyne devices.

Data Port Options Menu

For Data Port Options, refer to Table A-3. To access the Data Port Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → Data Port

Table A-3. Data Port Options (1 of 3)

Invert Transmit Clock
Possible Settings: **Enable, Disable** Default Setting: **Disable**
The DSU clock provided on Interchange Circuit CT114, Transmit Signal Element Timing DCE source (TXC), is phase inverted with respect to Interchange Circuit CT103, Transmitted Data (TXD). Recommended when data errors are occurring due to long cable lengths. **Enable** – The DSU-supplied clock is phase inverted with respect to TXD. **Disable** – The clock supplied by the DSU on TXC is normal (i.e., not inverted).
Port (DTE) Initiated Loopbacks
Possible Settings: **Disable**, **Local, Remote, Both** Default Setting: **Disable**
Specifies whether the DTE can initiate and terminate local and/or remote loopbacks. The DTE loopback control is done through the Interchange Circuits specified by the V.54 standard. NOTE: Refer to *Loopbacks* in Chapter 7. **Disable** – No local or remote loopbacks can be initiated by the DTE. **Local** – A local loopback can be controlled by the DTE, via the Interchange Circuit LL (CT141), as specified by V.54. The DTE port remains in loopback as along as LL remains on. Aborting the loopback from the ATI has no effect. **Remote** – A remote digital loopback can be controlled by the DTE, via Interchange Circuit RL (CT140), as specified by V.54. The remote equipment must be able to detect the in-band V.54 loopback sequence. **Both** – Both the local and remote loopbacks can be controlled by the DTE.
Bilateral Loopback
Possible Settings: **Enable, Disable** Default Setting: **Disable**
When a DSU loopback is initiated, a local DTE loopback is also automatically initiated. A Bilateral Loopback can be started by the ATI/NMS or by detection of a V.54 Loop 2 Up sequence. **Enable** – When Bilateral Loopback is enabled, running a DSU loopback also automatically starts a local loopback. The local loopback ends when the DSU loopback terminates. **Disable** – Running a DSU loopback does not start a local loopback. NOTE: Refer to *Loopbacks* and *Network Tests* in Chapter 7.

Table A-3. Data Port Options (2 of 3)

Carrier Control by RTS
Possible Settings: **Constant**, **Switched** Default Setting: **Constant**
Simulates Constant or Switched Carrier operation. ■ Carrier Control by RTS option can be changed only when In-Band Management Channel Rate (bps) is disabled (see Table A-2). **Constant** – The internal RTS is forced on and the DSU is in a constant Data Mode on the transmit line. The external RTS lead is ignored. The actual signal on the line is either all ones (DMI) or DTE transmitted data. **Switched** – RTS is monitored and CMI codes are transmitted when RTS is off.
CTS Control
Possible Settings: **Standard**, **Follow RTS, Forced On, Circuit Assurance** Default Setting: **Standard**
Specifies the operation of the Interchange Circuit CT106, Clear to Send (CTS), which is an output from the DSU. **Standard** – CTS follows the internal RTS with a fixed delay, except that CTS will be off when a network interface-related alarm is detected or a test is active. The active test may be initiated locally, remotely, or by the network. **Follow RTS** – CTS follows the external RTS lead without delay, regardless of alarms and tests. **Forced On** – CTS is always forced on after the unit is powered up with a successful self-test. **Circuit Assurance** – With circuit assurance, CTS operates the same as the Standard option, except that CTS will also be deasserted when CMI codes are being received.
RLSD Control
Possible Settings: **Standard**, **Forced On** Default Setting: **Standard**
Specifies the operation of the Interchange Circuit CT109, Received Line Signal Detector (RLSD or CD), which is an output from the DSU. **Standard** – RLSD is asserted when Data Mode is on the receive line. RLSD deasserts when a DDS facility alarm is detected or the DSU is receiving CMI codes. **Forced On** – RLSD is forced on after the unit is powered up with a successful self-test.
DSR Control
Possible Settings: **Standard**, **Forced On, On During Test** Default Setting: **Standard**
Specifies the operation of the Interchange Circuit CT107, Data Set Ready (DSR), which is an output from the DSU. **Standard** – DSR is always asserted, except when a DDS facility alarm is reported or the DSU is in Test mode. **Forced On** – DSR is forced on after the unit is powered up with a successful self-test. **On During Test** – DSU operates the same as the Standard option, except that DSR remains asserted when the DSU is in Test mode to allow the DTE to send test patterns.

Table A-3. Data Port Options (3 of 3)

Monitor DTR
Possible Settings: **Enable**, **Disable** Default Setting: **Enable**
Indicates to the DSU whether to monitor the Interchange Circuit CT108, Data Terminal Ready (DTR), from the DTE. **Enable** – The DSU monitors the state of DTR on the User Data (DTE) port. Based on the Link Traps option setting in Table A-9, the DSU uses the DTR circuit to trigger a Link Up/Down SNMP trap and a Health and Status message. **Disable** – DTR is not monitored by the DSU. Use when a DTE does not provide the DTR lead at the interface.

Ethernet Port Options Menu

For Ethernet Port Options, refer to Table A-4. To access the Ethernet Port Options screen, follow this menu selection sequence:

Main Menu → *Configuration* → *Load Configuration From* → *Edit* → *Ethernet Port*

Table A-4. Ethernet Port Options (1 of 2)

Port Use
Possible Settings: **802.3, Version 2, Disable** Default Setting: **Version 2**
The Ethernet port provides a choice of functions. **802.3** – Configures the DSU to use IEEE 802.3 format. **Version 2** – Configures the system to use Ethernet Version 2 format. **Disable** – Data received on this port is ignored. ■ No other fields in this table will appear when set to Disable.
IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the IP (Internet Protocol) address used to identify the Ethernet port. Each three-digit decimal number represents a byte. **000.000.000.000 – 223.255.255.255** – Enter an address. The range for the first byte is 000 to 223, with the exception of 127. The range for the remaining three bytes is 000 to 255. **Clear** – Clears the IP Address and sets to all zeros.

Table A-4. Ethernet Port Options (2 of 2)

IP Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask needed to access the Ethernet port. **000.000.000.000 – 255.255.255.255** – Set the Ethernet port subnet mask. The range for each byte is 000 to 255. **Clear** – Clears the subnet mask and sets to all zeros. When the subnet mask is all zeros, the device creates a default subnet mask based on the class of IP address: – Class A defaults to 255.000.000.000 – Class B defaults to 255.255.000.000 – Class C defaults to 255.255.255.000
Default Gateway Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the IP address of the default gateway to be used for packets that do not have a route. **000.000.000.000 – 223.255.255.255** – Enter an address. The range for the first byte is 000 to 223, with the exception of 127. The range for the remaining three bytes is 000 to 255. If the address is 000.000.000.000, all packets without a route are discarded. **Clear** – Clears the Default Gateway Address and sets to all zeros.

Terminal Port Options

For Terminal Port Options, refer to Table A-5. To access the Terminal Port Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → Terminal Port

Table A-5. Terminal Port Options (1 of 3)

Data Rate (Kbps)
Possible Settings: **2.4, 4.8, 9.6, 14.4, 19.2, 28.8, 38.4** Default Setting: **9.6**
Data rate in kbps on the Terminal port. **2.4 to 38.4** – Selects a Terminal port data rate from 2.4 to 38.4 kbps.
Character Length
Possible Settings: **7, 8** Default Setting: **8**
Specifies the number of bits needed to represent one character, including the parity bit. **7 or 8** – Sets the bits per character.

Table A-5. Terminal Port Options (2 of 3)

Parity
Possible Settings: **None, Even, Odd** Default Setting: **None**
Specifies Parity for the Terminal port. **None** – Provides no parity. **Even** – Parity is even. **Odd** – Parity is odd.
Stop Bits
Possible Settings: **1**, **2** Default Setting: **1**
Provides the number of stop bits for the Terminal port. **1** or **2** – Selects the number of stop bits.
Monitor DTR
Possible Settings: **Enable**, **Disable** Default Setting: **Enable**
Specifies monitoring of the Data Terminal Ready (DTR) control lead. **Enable** – Standard operation of the DTR control lead. **Disable** – DTR is ignored. Some external device connections may require this setting.
Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Used to secure access to the ATI through the Terminal port. Login IDs are created with a password and access level. **Enable** – Security is enabled. When ATI access is attempted through the Terminal port, a screen appears that requires a Login ID and password. **Disable** – Main menu appears with no Login required. NOTE: Refer to *Creating a Login* in Chapter 4.
Port Access Level
Possible Settings: **Level 1**, **Level 2, Level 3** Default Setting: **Level 1**
The Terminal port access level is interrelated with the access level of the Login ID. **Level 1** – This is the highest access level. If Login Required is disabled, the Terminal port access is level 1. If Login Required is enabled, the effective level is the Login ID access level. **Level 2** – This access level overrides a Login ID with an access level 1. If a Login ID has an access level of 3, the effective access level is 3. **Level 3** – This access level becomes the effective access level and overrides a Login ID with an access level of 1 or 2. NOTE: Refer to *ATI Access* in Chapter 4 for information about access levels.

Table A-5. Terminal Port Options (3 of 3)

Inactivity Timeout
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Provides automatic logoff of an ATI session through the Terminal Port. When the session is closed, User Interface Idle appears on the screen and the unit toggles the Terminal port DSR lead. **Enable** – The ATI session terminates automatically after the Disconnect Time set in the next option. When the session was occurring over an external modem connected to the Terminal port, the modem will interpret the DSR toggle as DTR being dropped and disconnect. **Disable** – An ATI session through the Terminal port will remain active indefinitely.
Disconnect Time(minutes)
Possible Settings: **range 1 – 60** Default Setting: **5**
Number of minutes of inactivity before the ATI session terminates automatically. Timeout is based on no keyboard activity. ■ Disconnect Time(minutes) option appears when Inactivity Timeout is enabled. **1 to 60** – The ATI user session is closed after the selected number of minutes.

Telnet Session Options

For Telnet Session Options, refer to Table A-6. To access the Telnet Session Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → Telnet Session

Table A-6. Telnet Session Options (1 of 2)

Telnet Session
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies if the DSU will respond to a Telnet session request from a Telnet client on an interconnected IP network. **Enable** – Allows Telnet sessions between the unit and a Telnet client. **Disable** – No Telnet sessions allowed.

Table A-6. Telnet Session Options (2 of 2)

Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Used to secure access to the ATI through a Telnet session. Login IDs are created with a password and access level. Refer to *Creating a Login* in Chapter 4. **Enable** – Security is enabled. When access is attempted via Telnet, the user is prompted for a Login ID and password. **Disable** – No Login required for a Telnet session.
Session Access Level
Possible Settings: **Level 1, Level 2, Level 3** Default Setting: **Level 1**
The Telnet session access level is interrelated with the access level of the Login ID. **Level 1** – This is the highest access level. Access level is determined by the Login ID. If Login Required is disabled, the session access is level 1. **Level 2** – This access level overrides a Login ID with an access level 1. If a Login ID has an access level of 3, the effective access level is 3. **Level 3** – This access level provides the effective access level and overrides a Login ID with an access level of 1 or 2. NOTE: Refer to *ATI Access* in Chapter 4 for information about access levels.
Inactivity Timeout
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Provides automatic logoff of a Telnet session. **Enable** – The Telnet session terminates automatically after the Disconnect Time set in the next option. **Disable** – A Telnet session will not be closed due to inactivity.
Disconnect Time (minutes)
Possible Settings: **range 1 – 60** Default Setting: **5**
Number of minutes of inactivity before a Telnet session terminates automatically. Timeout is based on no keyboard activity. ■ Disconnect Time (minutes) option appears when Inactivity Timeout is enabled. **1 to 60** – The Telnet session is closed after the selected number of minutes.

SNMP Menu

The SNMP Menu includes the following:

- General SNMP Management Options, Table A-7
- SNMP NMS Security Options, Table A-8
- SNMP Traps Options, Table A-9

General SNMP Management Options

For General SNMP Management Options, refer to Table A-7. To access the General SNMP Management Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → SNMP → General SNMP Management

Table A-7. General SNMP Management Options (1 of 2)

SNMP Management
Possible Settings: **Enable**, **Disable** Default Setting: **Disable**
Specifies if the DSU can be managed by an SNMP NMS. **Enable** – Enables SNMP management. **Disable** – DSU does not respond to SNMP messages.
Community Name 1
Possible Settings: **ASCII Text, Clear** Default Setting: **public**
Community Name of external SNMP Managers allowed access to the DSU's MIB. This community name must be supplied by an external SNMP manager attempting to access a MIB object. Level of access is set in the next option, Name 1 Access. **ASCII Text** – Enter a maximum of 130 ASCII printable characters. Refer to *Entering Device and System Information* in Chapter 3. **Clear** – Clears the Community Name 1 field.
Name 1 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Set the access level for the Community Name 1 created in the previous option. **Read** – Allows a read-only access (SNMP Get, Getnext) to accessible MIB objects. **Read/Write** – Allows SNMP Get, Getnext, and Set functions on MIB objects. Write access allowed to all MIB objects specified as read-write in the MIB RFC.

Table A-7. General SNMP Management Options (2 of 2)

Community Name 2
Possible Settings: **ASCII Text, Clear** Default Setting: [blank]
Community Name of external SNMP Managers allowed access to the DSU's MIB. This community name must be supplied by an external SNMP manager attempting to access a MIB object. Level of access is set in the next option, Name 2 Access. **ASCII Text** – Enter a maximum of 130 ASCII printable characters. Refer to *Entering Device and System Information* in Chapter 3. **Clear** – Clears the Community Name 2 field.
Name 2 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Set the access level for the Community Name 2 created in the previous option. **Read** – Allows a read-only access (SNMP Get, Getnext) to accessible MIB objects. **Read/Write** – Allows SNMP Get, Getnext, and Set functions on MIB objects. Write access allowed to all MIB objects specified as read-write in the MIB RFC.

SNMP NMS Security Options

For SNMP NMS Security Options, refer to Table A-8. To access the SNMP NMS Security Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → SNMP → SNMP NMS Security

Table A-8. SNMP NMS Security Options (1 of 2)

NMS IP Validation
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines if security checks are performed on the IP address of any SNMP management system that attempts to access the node. **Enable** – Performs security checking. Allows access only if the sending manager's IP address has been entered in the NMS IP address list. **Disable** – No security checking of incoming SNMP messages.
Number of Managers
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 10** Default Setting: **1**
Set the number of SNMP managers that are authorized to send SNMP messages. The IP address of each SNMP management system must be entered in the next option. **1 to 10** – Specifies the number of SNMP managers allowed to send SNMP messages.

Table A-8. SNMP NMS Security Options (2 of 2)

NMS *n* IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **000.000.000.000**
Enter an IP address for each of the managers set in the previous option. "*n*" is the number of the manager (1 to 10). Use the next option to establish the security level for each SNMP manager. NOTE: When an SNMP message is received from an IP address that does not match the IP address entries in this option, access is denied and, if SNMP traps are enabled, an "authenticationFailure" trap is generated. **000.000.000.000 – 223.255.255.255** – Sets the NMS IP address. The range for the first byte is 000 to 223, with the exception of 127. The range for the remaining three bytes is 000 to 255. **Clear** – Clears the IP address and sets to all zeros.
Access Level
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Set the access level for each IP address created in the previous option. **Read** – Allows read-only access (SNMP Get and Getnext) to accessible MIB objects. **Read/Write** – Allows an SNMP Get, Getnext, and Set to MIB objects. Write access allowed to all MIB objects specified as read-write in the MIB RFC. This access level is overridden by the Community Name's access level for the SNMP Manager, if the Community Name access level is Read.

SNMP Traps Options

For SNMP Traps Options, refer to Table A-9. To access the SNMP Traps Options screen, follow this menu selection sequence:

Main Menu → *Configuration* → *Load Configuration From* → *Edit* → *SNMP* → *SNMP Traps*

Table A-9. SNMP Traps Options (1 of 2)

SNMP Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Controls the generation of SNMP trap messages. The options for addresses and types of traps are located in this table. ■ SNMP Management must be enabled. See Table A-7. **Enable** – SNMP trap messages are sent out to SNMP managers. **Disable** – No SNMP trap messages are sent out.
Number of Trap Managers
Possible Settings: **1, 2, 3, 4, 5, 6** Default Setting: **1**
Sets the number of SNMP management systems that will receive SNMP traps. **1 to 6** – Number of trap managers. An NMS IP address is required for each manager.
Trap Manager *n* IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the IP address used to identify each SNMP trap manager. *n* represents the number of the manager (from 1 to 6). **000.000.000.000 – 223.255.255.255** – Enter an address for each SNMP trap manager. The range for the first byte is 000 to 223, with the exception of 127. The range for the remaining three bytes is 000 to 255. **Clear** – Clears the IP address and sets to all zeros.
Trap Manager *n* Destination
Possible Settings: **None, Ethernet, IMC** Default Setting: **None**
Provides the network destination path of each trap manager. *n* is the number of the manager (from 1 to 6). **None** – No destination is specified for Trap Manager *n*. **Ethernet** – Ethernet port is the network destination. ■ Port Use option must not be set to Disable. See Table A-4. **IMC** – The In-Band Management Channel is the default network destination. ■ In-Band Management Channel Rate (bps) option must be set to 1600, 4000, or 8000 bps. See Table A-2.

Table A-9. SNMP Traps Options (2 of 2)

General Traps
Possible Settings: **Disable, Warm, AuthFail, Both** Default Setting: **Both**
Determines which SNMP traps are sent to each trap manager. **Disable** – No general trap messages are sent. **Warm** – Sends trap message for "*warmStart*". **AuthFail** – Sends trap message for "*authenticationFailure*". **Both** – Sends both trap messages. NOTE: Refer to Appendix D, *Standards Compliance for SNMP Traps*.
Enterprise Specific Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
This option is used to determine if SNMP traps are generated for enterprise-specific events. **Enable** – SNMP traps are generated for enterprise-specific events. NOTE: Refer to *Traps: enterpriseSpecific* in Appendix D. **Disable** – No enterprise-specific event traps are sent.
Link Traps
Possible Settings: **Disable, Up, Down, Both** Default Setting: **Both**
This option is used to determine if SNMP traps are generated for link up and link down for one of the communication interfaces. **Disable** – No linkUp or linkDown SNMP traps are generated. **Up** – A linkUp trap is generated when the DSU recognizes that one of the communication interfaces is operational. **Down** – A linkDown trap is generated when the DSU recognizes a failure in one of the communication interfaces. **Both** – Sends trap messages for detection of both linkUp and linkDown. NOTE: Refer to *Traps: linkUp and linkDown* in Appendix D.
Link Trap Interfaces
Possible Settings: **Network, Port, Both** Default Setting: **Both**
This option determines if the SNMP linkUp, SNMP linkDown, and interface-related enterprise-specific traps are generated for the DDS Network Interface and/or User Data (DTE) port. NOTE: These traps are not supported on the Terminal port. **Network** – SNMP trap messages are generated for the DDS network interface. **Port** – SNMP trap messages are generated for the User Data (DTE) port. **Both** – SNMP trap messages are generated on both the DDS network interface and the User Date (DTE) port.

Worksheets

B

Overview

The worksheets in this appendix summarize the configuration options accessed when you select Configuration on the Main Menu. The possible menu selections are displayed with the default settings and the possible settings.

Configuration Worksheets

System	
Configuration Option	**Settings** *Default in [**Bold**]*
Operating Mode	[**DDS**], LADS
DDS Line Rate (Kbps)	56, 64CC, [**Autobaud**]
LADS Timing	[**Internal**], External, Receive
LADS Line Rate (Kbps)	56, [**64**]
Test Timeout	[**Enable**], Disable
Test Duration (min)	1–120 [**10**]

Network Interface	
Configuration Option	**Settings** *Default in [**Bold**]*
Network-initiated DSU Loopback (64K CC)	[**Enable**], Disable
Data Scrambling (64K CC)	Enable, [**Disable**]
V.54 Initiated DSU Loopback	Enable, [**Disable**]
In-Band Management Channel Rate (bps)	[**Disable**], 1600, 4000, 8000
IMC IP Address	[**000.000.000.000**] – 223.255.255.255
IMC Subnet Mask	[**000.000.000.000**] – 255.255.255.255
IMC Routing Information Protocol	None, [**Proprietary**]

Data Port	
Configuration Option	**Settings** *Default in [**Bold**]*
Invert Transmit Clock	Enable, [**Disable**]
Port (DTE) Initiated Loopbacks	[**Disable**], Local, Remote, Both
Bilateral Loopback	Enable, [**Disable**]
Carrier Control by RTS	[**Constant**], Switched
CTS Control	[**Standard**], Follow RTS, Forced On, Circuit Assurance
RLSD Control	[**Standard**], Forced On
DSR Control	[**Standard**], Forced On, On During Test
Monitor DTR	[**Enable**], Disable

Ethernet Port	
Configuration Option	**Settings** *Default in [**Bold**]*
Port Use	802.3, **Version 2**, Disable
IP Address	[**000.000.000.000**] – 223.255.255.255
IP Subnet Mask	**[000.000.000.000]** – 255.255.255.255
Default Gateway Address	[**000.000.000.000**] – 223.255.255.255

Terminal Port	
Configuration Option	**Settings** *Default in [**Bold**]*
Data Rate (Kbps)	2.4, 4.8, [**9.6**], 14.4, 19.2, 28.8, 38.4
Character Length	7, [**8**]
Parity	[**None**], Even, Odd
Stop Bits	[**1**], 2
Monitor DTR	[**Enable**], Disable
Login Required	Enable, [**Disable**]
Port Access Level	[**Level 1**], Level 2, Level 3
Inactivity Timeout	Enable, [**Disable**]
Disconnect Time(minutes)	range 1 – 60 [**5**]

Telnet Session	
Configuration Option	**Settings** *Default in [**Bold**]*
Telnet Session	Enable, [**Disable**]
Login Required	Enable, [**Disable**]
Session Access Level	[**Level 1**], Level 2, Level 3
Inactivity Timeout	Enable, [**Disable**]
Disconnect Time(minutes)	range 1 – 60 [**5**]

SNMP	
Configuration Option	**Settings** *Default in [**Bold**]*
General SNMP Management	
SNMP Management	Enable, [**Disable**]
Community Name 1	ASCII Text, **[public**]
Name 1 Access	[**Read**], Read/Write
Community Name 2	ASCII Text, [*blank*]
Name 2 Access	[**Read**], Read/Write
SNMP NMS Security	
NMS IP Validation	Enable, [**Disable**]
Number of Managers	[**1**], 2, 3, 4, 5, 6, 7, 8, 9, 10
NMS *n* IP Address	[**000.000.000.000**] – 223.255.255.255
Access Level	[**Read**], Read/Write
SNMP Traps	
SNMP Traps	Enable, [**Disable**]
Number of Trap Managers	[**1**], 2, 3, 4, 5, 6
Trap Manager *n* IP Address	[**000.000.000.000**] – 223.255.255.255
Trap Manager *n* Destination	[**None**], Ethernet, IMC
General Traps	Disable, Warm, AuthFail, [**Both**]
Enterprise Specific Traps	Enable, [**Disable**]
Link Traps	Disable, Up, Down, [**Both**]
Link Trap Interfaces	Network, Port, [**Both**]

MIB Descriptions

C

Overview

The following sections show how the 7612 SNMP DSU supports MIB objects relative to their RFC descriptions. MIBs are available on the World Wide Web site listed on Page A (the reverse side of the title page of this document). The 7612 SNMP DSU supports:

- MIB II (see below)
- RS-232-Like MIB (see page C-13)
- Ethernet-Like MIB (see page C-17)
- Paradyne Enterprise MIB (see page C-17)

MIB II – RFC 1213 and RFC 1573

The unit supports the following MIB II object groups as defined in RFC 1213 and RFC 1573:

- System Group Objects
- Interfaces Group Objects – Supported for the DDS network interface, DTE port, Terminal port, 10BaseT port, and the IMC as defined in RFC 1573, the Evolution of the Interfaces Group.
  - Interfaces Group Objects
  - Extension to Interface Table (ifXTable)
  - Interface Stack Group Objects
  - Interface Test Group Objects
- IP Group Objects
- ICMP (Internet Control Management Protocol) Group
- TCP (Transmission Control Protocol) Group
- UDP (User Datagram Protocol) Group

- Transmission Group Objects. Supported on the:
  - — DDS network interface using the DDS Enterprise MIB.
  - — User Data (DTE) port and Terminal port using the RS-232-like MIB.
  - — 10BaseT port using the Ethernet-like MIB.
- SNMP Group

The following MIB II groups are not supported:

- Address Translation Group
- Exterior Gateway Protocol (EGP) Group

System Group

System Group objects are fully supported by the unit, as shown in Table C-1.

Table C-1. System Group Objects

Object	Description	Setting/Contents
sysDescr *(system 1)*	Provides a full name and version identification for the system's hardware and software.	PARADYNE DDS Leased Line DSU*;* Model: 7612-A1-201; S/W Release: *yy.yy.yy;* H/W Revision: *zzzz-zzz;* Serial Number: *sssssss*
sysObjectID *(system 2)*	Identifies the network management subsystem.	1.3.6.1.4.1.1795.1.14.2.5.1.1
sysContact *(system 4)*	Provides the textual identification of the contact person for this managed unit.[1]	ASCII character string, as set by the user.
sysName *(system 5)*	Provides an administrative assigned name for this managed unit.[1]	ASCII character string, as set by the user.
sysLocation *(system 6)*	Provides the physical location for this managed unit.[1]	ASCII character string, as set by the user.
sysServices *(system 7)*	Functionality supported: ■ **physical (1)** – Layer 1 functionality for all interfaces. ■ **datalink/subnetwork (2)** – Layer 2 functionality (PPP) for all management links. ■ **internet (4)** – Layer 3 functionality (IP) for all management links. ■ **end-to-end (8)** – Layer 4 functionality (TCP/UDP) for all management links.	Object is set to 1+2+4+8 (**15**).

[1] The unit supports a 127-character string for this object. An error message is sent to the NMS if an attempt is made to write (set) more than 127 characters.

Interfaces Group

The Interfaces Group as defined in RFC 1573 consists of an object indicating the number of interfaces supported by the unit and an interface table containing an entry for each interface. Since RFC 1573 is an SNMPv2 MIB, it is converted to SNMPv1 for support by the unit. Table C-2 provides clarification for objects contained in the Interfaces group when it is not clear how the object definition in RFC 1573 is supported by the unit.

Table C-2. Interfaces Group Objects (1 of 4)

Object	Description	Setting/Contents
ifNumber *(interfaces 1)*	Specifies the number of interfaces for this unit in the ifTable.	**5**
ifIndex *(ifEntry 1)*	Provides the index to the interface table (ifTable) and to other tables as well. When an unsupported index is entered (e.g., 1 and 5), noSuchName is returned.	Indexes and values: **1** – reserved **2** – Terminal port **3** – Ethernet port **4** – DDS network interface **5** – reserved **6** – User Data (DTE) port **7** – In-band Management Channel
ifDescr *(ifEntry 2)*	Supplies text for each Interface:	Text Strings for each interface:
	■ Terminal	■ "Terminal Port; PARADYNE DDS Leased Line DSU; Hardware Version [*Hardware Revision*]"; Software Version: [*Software Revision*].
	■ Ethernet	■ "Ethernet Port; PARADYNE DDS Leased Line DSU; Hardware Version [*Hardware Revision*]"; Software Version: [*Software Revision*].
	■ DDS Network	■ "DDS Network; PARADYNE DDS Leased Line DSU; Hardware Version [*Hardware Revision*]"; Software Version: [*Software Revision*].
	■ User Data Port	■ "User Data Port; PARADYNE DDS Leased Line DSU; Hardware Version [*Hardware Revision*]"; Software Version: [*Software Revision*].
	■ In-band Management Channel	■ "In-band Management Channel; PARADYNE DDS Leased Line DSU; Hardware Version [*Hardware Revision*]"; Software Version: [*Software Revision*].

Table C-2. Interfaces Group Objects (2 of 4)

Object	Description	Setting/Contents
ifType *(ifEntry 3)*	Identifies the interface type based on the physical/link protocol(s), right below the network layer.	Supported values: ■ **ethernetCsmacd(6)** – Used for the Ethernet port. ■ **other(1)** – Used for the DDS network. ■ **ppp(23)** – Used for the In-band Management Channel. ■ **rs232(33)** – Used for the Terminal port. ■ **v35(45)** – Used for the User Data port.
ifMtu *(ifEntry 4)*	Identifies the largest datagram that can be sent or received on an interface (Ethernet port or IMC).	Number of octets.
ifSpeed *(ifEntry 5)*	Provides the current bandwidth for the interface in bits per second.	■ Ethernet Port – The data rate for the port. ■ Terminal port – Configured data rate for the port. ■ DDS – Line rate of 56,000 or 64,000 bps, reflecting the line rate detected by the unit. ■ User data (DTE) port – Current data rate of the port (DDS operating rate minus IMC rate). ■ In-band Management Channel – Configured data rate for the In-band Management Channel.
ifAdminStatus *(ifEntry 7)*	Provides interface status. Supported as read-only.	■ **up(1)** – The interface is enabled. ■ **down(2)** – The interface is disabled.

Table C-2. Interfaces Group Objects (3 of 4)

Object	Description	Setting/Contents
ifOperStatus *(ifEntry 8)*	Specifies the current operational state of the interface.	■ Ethernet port – **up(1)** – No alarms – **down(2)** – Alarms – **testing(3)** – Test active ■ Terminal port. Always **up(1)**; never in **testing(3)** state. ■ User Data Port – **up(1)** – No alarms – **down(2)** – Alarms – **testing(3)** – Test active ■ DDS Network Interface – **up(1)** – DTR on, if supported by the DTE – **down(2)** – DTR off, if supported by the DTE – **testing(3)** – Test active ■ In-band Management Channel. When enabled, up and down are based on the current state of the physical and link layer protocols. – **up(1)** – Operational and no active test on the DDS network interface – **down(2)** – Not operational or disabled – **testing(3)** – Test active on DDS network interface
ifLastChange *(ifEntry 9)*	Indicates the amount of time the interface has been up and running.	Contains the value of sysUpTime object at the time the interface entered its current operational state.
ifInOctets *(ifEntry 10)*	Collects input statistics on data received by the interface. Applies to the IMC and the Ethernet port. Statistics are not collected if the Ethernet port is disabled.	An integer number.
ifInUcastPkts *(ifEntry 11)*		
ifInDiscards *(ifEntry 13)*		
ifInErrors *(ifEntry 14)*		
ifInUnknown Protos *(ifEntry 15)*		

Table C-2. Interfaces Group Objects (4 of 4)

Object	Description	Setting/Contents
ifOutOctets *(ifEntry 16)*	Collects output statistics on data received by the interface. Applies to the IMC and the Ethernet port. Statistics are not collected if the Ethernet port is disabled.	An integer number.
ifOutUcastPkts *(ifEntry 17)*		
ifOutDiscards *(ifEntry 19)*		
ifOutErrors *(ifEntry 20)*		

Extension to Interface Table (ifXTable)

This extension contains additional objects for the Interface table. Table C-3 shows the objects supported.

Table C-3. Extension to Interface Table (ifXTable)

Object	Description	Setting/Contents
ifName *(ifXEntry 1)*	Provides name of the interface.	Interface text strings: ■ Ethernet Port ■ Terminal Port ■ DDS Network ■ User Data Port ■ In-band Management Channel
ifLinkUpDown-TrapEnable *(ifXEntry 14)*	Indicates whether the link is up or down, or enterprise-specific traps should be generated.	Only supports DDS network and User data port. SNMP Traps must be enabled for the unit. See Table A-9, SNMP Traps Options.
ifHighSpeed *(ifXEntry 15)*	Reflects the ifSpeed setting for the interface.	This object is supported as read-only.
ifConnector-Present *(ifXEntry 17)*	Indicates whether there is a physical connector for the interface.	**true(1)** – Will always have this value for the DDS network, Ethernet port, Terminal port, and User Data port. **false(2)** –Will always have this value for the In-band Management Channel.

Interface Stack Group

The Interface Stack Group is used by the unit to show the relationship between a logical interface and a physical interface. Table C-4 provides clarification for objects contained in the Interface Stack group when it is not clear how the object definition in RFC 1573 is supported by the unit.

Table C-4. Interface Stack Group Objects

Object	Description	Setting/Contents
ifStackHigher-Layer *(ifStackEntry1)*	Provides the index that corresponds to the higher sublevel specified by ifStackLowerLayer.	When the In-band Management Channel is enabled, this object for the DDS network interface is set to the ifIndex of the In-band Management Channel. All other ifStackHigherLayer objects will have a value of zero.
ifStackLower-Layer *(ifStackEntry2)*	Provides the index that corresponds to the lower sublevel specified by ifStackHigherLayer.	When the In-band Management Channel is enabled, this object for the In-band Management Channel is set to the ifIndex of the DDS network interface. All other ifStackLowerLayer objects will have a value of zero.
ifStackStatus *(ifStackEntry3)*	Specifies the stack group's status compared to the interface's ifOperStatus. Supported as a read-only variable.	■ When ifStackStatus set to **active** – maps to ifOperStatus set to **up(1)** or **testing(3)**. ■ When ifStackStatus set to **not in service** – maps to ifOperStatus set to **down(2)**.

Interface Test Table

The unit uses the Interface Test table to provide access to additional tests such as loopbacks and pattern tests, which are not included in the Interfaces Group of MIB II. Interface Test Group objects are shown in Table C-5.

Table C-5. Interface Test Group Objects (1 of 2)

Object	Description	Setting/Contents
ifTestID *(ifTestEntry 1)*	Provides a unique identifier for the current request of the interface's test. Ensures that the results of the test are for that request. This handles the rare condition where another SNMP Manager starts a test immediately after completion of a previous test, but before the previous test results are received by the first SNMP manager.	Set by an SNMP Manager before the test is started. The unit then increments the previous value. The value is then checked after the test has completed.
ifTestStatus *(ifTestEntry2)*	Indicates the test status of the interface.	■ Set to **inUse(2)** by an SNMP Manager before a test is started. ■ Set to **notInUse(1)** by the unit when the test has completed. Also set to **notInUse(1)** by the unit if the SNMP Manager fails to set an ifTestType within 5 minutes.
ifTestType *(ifTestEntry 3)*	A control variable used to start/stop user-initiated tests on the interface. Provides the following capabilities: ■ Start/stop user data port loopback ■ Start/stop send pattern on the user data port ■ Start/stop the monitor test pattern on the user data port	The following objects use identifiers to control tests on the User Data port interface: ■ **noTest** (0 0) – Stops the test in progress on the interface. ■ **testLoopDTE** (ifTestType 2) – Starts a Local Loopback (DTE) on the interface. ■ **testMon511** (ifTestType 4) – Starts a Monitor 511 test on the interface. ■ **testSend511** (ifTestType 6) – Starts a Send 511 test on the interface.

Table C-5. Interface Test Group Objects (2 of 2)

Object	Description	Setting/Contents
ifTestCode *(ifTestEntry 5)*	Contains a code which is more specific about the test results.	Supports the following values: ■ **none** (ifTestCode 1) – No further information is available. Used for send pattern/code and loopback tests. ■ **inSyncNoBitErrors** (ifTestCode 2) – A 511 monitor pattern test has synchronized on the pattern and has not detected any bit errors. ■ **inSyncWithBitErrors** (ifTestCode 3) – A 511 monitor pattern test has synchronized on the pattern and has detected bit errors. ■ **notInSync** (ifTestCode 4) – A 511 monitor test pattern has not synchronized on the requested pattern.
ifTestOwner *(ifTestEntry 6)*	Used by an SNMP Manager to identify the current owner of the test for the interface.	The SNMP Manager sets the object to its IP address when setting ifTestID and ifTestStatus.

Generic Receive Address Table

Not supported by the unit.

IP Group

The Internet Protocol Group objects are supported by the unit for all data paths that are currently configured to carry IP data to/from the unit. All of the objects in the IP Group, except for the IP Address Translation table, are fully supported. Table C-6 provides clarification for objects contained in the IP group when it is not clear how the object definition in MIB II is supported by the unit.

Table C-6. IP Group Objects (1 of 2)

Object	Description	Setting/Contents
ipForwarding *(ip1)*	Specifies whether the unit is acting as an IP gateway for forwarding of datagram received by, but not addressed to, the unit.	Supports only the following value: ■ **forwarding(1)** – The unit is acting as a gateway.
ipAddrTable *(ip20)*	The address table.	Supported.
ipAdEntAddr *(ipAddrEntry 1)*	An IP address supported by the unit which serves as an index to the address table.	Indexes for tables must be unique. Therefore, only one ifIndex can be displayed for each IP address supported by the device. If the same IP address is configured for multiple interfaces, or for default IP addresses, the ipAddrTable will not display all of the interfaces that support a particular IP address.
ipAdEntIfIndex *(ipAddrEntry 2)*	If this object has a greater value than the ifNumber, then it refers to a proprietary interface not currently implemented by the MIB II Interface Group.	None
ipRouteTable *(ip21)*	Supported as read/write. However, use caution when adding or modifying routes. If it is absolutely necessary to add a route, the route should only be added to the connected device (device closest to the destination). Internal routing will continue the route to the other devices.	To delete a route, set object to **invalid**. To modify a route, change fields in the desired entry of the routing table (indexed by ipRouteDest). To add a route, specify values for a table entry for which the index (ipRouteDest) does not already exist. The following objects *must* be specified: ■ ipRouteDest – Serves as an index to the routing table. Only one route per destination can appear in the table. To ensure that no duplicate destinations appear in the routing table, the ipRouteDest object will be treated as described in the IP Forwarding Table MIB (RFC 1354).

Table C-6. IP Group Objects (2 of 2)

Object	Description	Setting/Contents
ipRouteTable *(ip21)* (Continued)		■ ipRouteIfIndex – If this object has a greater value than the ifNumber, then it refers to a proprietary interface not currently implemented by the MIB II Interface Group. Do not delete route entries with an unrecognized ipRouteIfIndex. When setting this object via SNMP, the ipRouteIfIndex value can only assume an appropriate value of IfIndex defined for a particular device type. Objects that will be set to the default value if not specified in the Set PDU used to add a route: ■ ipRouteMetric1 – Defaults to 1 hop. ■ ipRouteType – Defaults to indirect. ■ ipRouteMask – Defaults to what is specified in the MIB description. Objects that are not used by this unit: ■ ipRouteMetric2, ipRouteMetric3, ipRoutemetric4, ipRoutemetric5 – Default to **–1**. ■ ipRouteNextHop – Defaults to **0.0.0.0**. Do not specify the following read-only objects in the Set PDU used to add a route: ■ ipRouteProto – Set to **netmgmt(3**) by the software. May have the following values: – **other(1)** – Temporary route added by IP. – **local(2)** – Route added or changed due to User configuration. – **netmgmt(3)** – Route added or changed by SNMP set. – **icmp(4)** – Route added or changed by ICMP. – **rip(8)** – Route added or changed by RIP (or similar proprietary protocol). ■ ipRouteAge – Reflects the value of the time-to-live for the route (in seconds). Defaults to **999** (permanent route). ■ ipRouteInfo – Unused; set to {0, 0}.

ICMP Group

The ICMP (Internet Control Management Protocol) Group objects are fully supported.

TCP Group

The TCP Group objects are fully supported, with the exception of tcpConnState object, which will be read-only, since deleteTCB (12) is not supported and is the only value which can be set.

UDP Group

The UDP Group objects are fully supported.

Transmission Group

Objects in the Transmission Group are supported on the DDS network interface, User Data port, Ethernet port, and Terminal port. These objects are defined through other Internet-standard MIB definitions rather than within MIB II. Table C-7 shows how Transmission Group objects are supported.

Table C-7. Transmission Group Objects

Object	Description
dot3 *(transmission 7)*	Supported on the Ethernet port. Defined by the Ethernet-like MIB (RFC 1643).
rs232 *(transmission 33)*	Supported on the User Data port and Terminal port. Defined by the RS-232-like MIB (RFC 1659).
enterprise *(transmission 22)*	Supported on the DDS network interface by Paradyne Enterprise MIB.

SNMP Group

The SNMP Group objects that apply to a management agent are fully supported. The following objects apply only to an NMS and return a zero value if accessed.

- snmpInTooBig (snmp 8)
- snmpInNoSuchNames (snmp 9)
- snmpInBadValues (snmp 10)
- snmpInReadOnlys (snmp 11)
- snmpInGenErrs (snmp 12)
- snmpInGetResponses (snmp 18)

- snmpInTraps (snmp 19)
- snmpOutGetRequests (snmp 25)
- snmpOutGetNexts (snmp 26)
- snmpOutSetRequests (snmp 27)

RS-232-Like MIB, RFC 1659

Supported for the User Data port and the Terminal port. RFC 1659 is an SNMPv2 MIB, but is converted to an SNMPv1 MIB to support this unit. This MIB consists of one object and five tables.

- Number of RS-232-Like Ports Object.
- General Port Table Objects.
- Asynchronous Port Table Objects. Not supported for the User Data port.
- Synchronous Port Table Objects. Not supported for the Terminal port.
- Input Signal Table Objects. Not supported for the Terminal port.
- Output Signal Table Objects. Not supported for the Terminal port.

Number of RS-232-Like Ports Object

Supported as documented in the RFC.

General Port Table Objects

The General Port Table Objects contains configuration options for the RS-232-Like interfaces. Clarification for objects contained in Table C-8 as it applies to the unit is provided below.

Table C-8. General Port Table Objects (1 of 2)

Object	Description	Setting/Contents
rs232PortType *(rs232PortEntry 2)*	Identifies the port hardware type.	Supports only the following values: **rs232(2)** – Identifies the Terminal port. **v35(5)** – Identifies the synchronous User Data port which is compatible with the V.35 standard.
rs232PortInSig Number *(rs232PortEntry 3)*	Contains the number of input signals (in the input signal table) that can be detected.	The value is **2** for synchronous user data port and **0** for the Terminal port.

Table C-8. General Port Table Objects (2 of 2)

Object	Description	Setting/Contents
rs232PortOutSig Number *(rs232PortEntry 4)*	Contains the number of output signals (in the output signal table) that can be asserted.	The value is **3** for synchronous User Data port and **0** for the Terminal port.
rs232PortInSpeed *(rs232PortEntry 5)*	Contains the port's input speed in bits per second.	Supports the following speeds for the: ■ User data port: 64,000, 62,400, 60,000, 56,000, 54,400, 52,000, 48,000.[1] ■ Terminal port: 2400, 4800, 9600,14,400, 19,200, 28,800, 38,400.
rs232PortOut Speed *(rs232PortEntry 6)*	Contains the port's output speed in bits per second. The rs232PortOutSpeed object has the same values as the rs232PortInSpeed object.	Supports the following speeds for the: ■ User data port: 64,000, 62,400, 60,000, 56,000, 54,400, 52,000, 48,000.[1] ■ Terminal port: 2400, 4800, 9600,14,400, 19,200, 28,800, 38,400.
[1] The User Data port speed is a read-only value that can only differ from the DDS network speed if the In-band Management Channel is enabled.		

The following are not supported:

- rs232PortInFlowType *(rs232PortEntry 7)*
- rs232PortOutFlowType *(rs232PortEntry 8)*

Asynchronous Port Table Objects

The Asynchronous Port Table contains an entry for the Management port when the port is configured for asynchronous operation and for the Terminal port. For this unit, entries in the table that are counters (rs232AsyncPortEntry 6–8) are used to collect statistics only and are not supported. Table C-9 shows the Asynchronous Port Table objects supported.

Table C-9. Asynchronous Port Table Objects (1 of 2)

Object	Description	Setting/Contents
rs232AsyncPort Bits *(rs232Async PortEntry 2)*	Specifies the number of bits in a character.	Supports only the following values: **7** – 7-bit characters **8** – 8-bit characters
rs232AsyncPort StopBits *(rs232Async PortEntry 3)*	Specifies the number of stop bits supported.	Supports only the following values: **one(1)** – One stop bit **two(2)** – Two stop bits

Table C-9. Asynchronous Port Table Objects (2 of 2)

Object	Description	Setting/Contents
rs232AsyncPort Parity *(rs232Async PortEntry 4)*	Specifies the type of parity used by the port.	Supports only the following values: **none(1)** – No parity bit **odd(2)** – Odd parity **even(3)** – Even parity
rs232AsyncPort AutoBaud *(rs232Async PortEntry 5)*	Specifies the ability to automatically sense the input speed of the port.	Supports only the following value: **disabled(2)** – Does not support Autobaud.

Synchronous Port Table Objects

The Synchronous Port Table contains an entry for the synchronous user data port when this port is configured for synchronous operation. For this unit, entries in the table that are counters (rs232SyncPortEntry 3–7) are used to collect statistics only and are not supported. Clarification for objects contained in this table as it applies to the unit is provided in Table C-10.

Table C-10. Synchronous Port Table Objects (1 of 2)

Object	Description	Setting/Contents
rs232SyncPort Role *(rs232Sync PortEntry 8)*	Specifies whether this device interface is a DTE or DCE.	Supports only the following value: **dce(2)** – The port acts as a DCE.
rs232SyncPort Encoding *(rs232Sync PortEntry 9)*	Specifies the bit encoding technique that this port uses.	Supports only the following value: **nrz(1)** – The port uses non-return to zero encoding.
rs232SyncPort RTSControl *(rs232Sync PortEntry 10)*	Specifies the method used to control the RTS signal. Refer to Data Port Options, Table A-3.	Supports only the following values: **controlled(1)** – For User Data port, this value is used when the Data Port option Carrier Control by RTS is set to Switched. **constant(2)** – For User Data port, this value is used when the Data Port option Carrier Control by RTS is set to Constant.

Table C-10. Synchronous Port Table Objects (2 of 2)

Object	Description	Setting/Contents
rs232SyncPort RTSCTSDelay *(rs232Sync PortEntry 11)*	Reports the interval (in milliseconds) that the port waits after RTS is asserted before asserting CTS.	Supports only the following read-only value: **integer number** – represents milliseconds. It is only valid for the user data port, when Carrier Control by RTS is set to Switched and corresponds to approximately 21 bit time intervals at the operating DDS rate.
rs232SyncPort Mode *(rs232Sync PortEntry 12)*	Specifies the port's mode of data transfer.	Supports only the following value: **fdx(1)** – Full-duplex

The following are not supported:

- rs232SyncPortIdle Pattern *(rs232SyncPortEntry 13)*
- rs232SyncPortMinFlags *(rs232SyncPortEntry 14)*

Input Signal Table Objects

The Input Signal Table contains entries for the input signals that can be detected by the unit for the synchronous user data port. Clarification for objects contained in this table as it applies to the unit is provided in Table C-11.

Table C-11. Input Signal Table Objects

Object	Description	Setting/Contents
rs232InSigName *(rs232InSigEntry 2)*	Contains the identification of a hardware input signal.	Supports only the following values: **rts(1)** – Request To Send **dtr(4)** – Data Terminal Ready
rs232InSigState *(rs232InSigEntry 3)*	Contains the current signal state.	Supports only the following values: **on(2)** – The signal is asserted **off(3)** – The signal is deasserted
rs232InSigChanges *(rs232InSigEntry 4)*	Indicates the number of times that a signal has changed from on to off, or off to on.	The object is incremented each time that the signal is sampled (every 100 ms) and the signal state is different from the previous state.

Output Signal Table Objects

The Output Signal Table contains entries for the output signals that can be asserted by the unit, for the synchronous User Data port. Clarification for objects contained in this table as it applies to the unit is provided in Table C-12.

Table C-12. Output Signal Table Objects

Object	Description	Setting/Contents
rs232OutSigName *(rs232OutSigEntry 2)*	Contains the identification of a hardware output signal.	Supports only the following values: **cts(2)** – Clear To Send **dsr(3)** – Data Set Ready **dcd(6)** – Received Line Signal Detector
rs232OutSigState *(rs232OutSigEntry 3)*	Contains the current signal state.	Supports only the following values: **on(2)** – The signal is asserted **off(3)** – The signal is deasserted
rs232OutSigChanges *(rs232OutSigEntry 4)*	Indicates the number of times that a signal has changed from on to off, or off to on.	Increments the object each time that the signal is sampled (every 100 ms) and the signal state is different from the previous state.

Ethernet-Like MIB, RFC 1643

The unit supports the Ethernet-Like MIB, RFC 1643 for all objects *except*:

- dot3TestTdr, and
- dot3StatsEtherChipSet

Enterprise MIB

The following Paradyne Enterprise MIB Objects are supported by the unit:

- Device Configuration Variable (pdn-dev Config 7)
- Port Usage Table, pdn-devPortUsage (pdn-interfaces 3)
- DDS Interface Specific Definitions, pdn-dds (pdn-interfaces 2)
- Device Security, pdn-security (pdn-common 8)
- Device Traps, pdn-traps pdn-common 9)
- Device Control, pdn-control (pdn-common 10)

Device Configuration Variable (pdn-common 7)

The variable devConfigAreaCopy in the devConfigArea group is supported. This variable allows the entire contents of one configuration area to be copied into another configuration area. The unit only supports the values shown in Table C-13.

Table C-13. Device Configuration Variable

Object	Description	Setting/Contents
devConfig AreaCopy	A “get” of this object will always return noOp.	**noOp(1)**
	Copy from active area to customer 1 area.	**active-to-customer1(2)**
	Copy from active area to customer 2 area.	**active-to-customer2(3)**
	Copy from customer 1 area to active area.	**customer1-to-active(4)**
	Copy from customer 1 area to customer 2 area.	**customer1-to-customer2(5)**
	Copy from customer 2 area to active area.	**customer2-to-active(6)**
	Copy from customer 2 area to customer 1 area.	**customer2-to-customer1(7)**
	Copy from factory area to active area. There is only one factory area for the unit.	**factory1-to-active(8)**
	Copy from factory area to customer 1 area.	**factory1-to-customer1(9)**
	Copy from factory area to customer 2 area.	**factory1-to-customer2(10)**

DDS Interface Specific Definitions, pdn-dds (pdn-interfaces 2)

The DDS Interface Specific Definitions contain objects that are used to manage the DDS Network Interface. The unit supports all objects except the ASCII alarms.

Device Security, pdn-security (pdn-common 8)

Use the Device Security table to control the number of SNMP managers that may access the unit, as well as the unit access level (read or read/write). Fully supported by the unit.

Device Traps, pdn-traps (pdn-common 9)

Controls the SNMP managers to which the unit reports traps. Fully supported by the unit.

Device Control, pdn-control (pdn-common 10)

Uses the devControlReset object to reset the unit. Fully supported by the unit.

Standards Compliance for SNMP Traps

D

Overview

This appendix describes the unit's compliance with SNMP standards and any special operational features for the SNMP traps supported. The unit supports user interface traps and enterprise-specific traps.

Trap: warmStart

SNMP Trap	Description	Possible Cause
warmStart	The unit has reinitialized itself. The trap is sent after the unit resets itself and stabilizes. There are no variable-bindings.	■ Reset command. ■ Power disruption.

Trap: authentificationFailure

SNMP Trap	Description	Possible Cause
authenticationFailure	Failed attempts to access the unit. There are no variable-bindings.	■ SNMP message not properly authenticated. ■ Three unsuccessful attempts were made to enter a correct login/password combination. ■ IP address security is enabled, and a message was received from SNMP manager whose address was not on the list of approved managers.

Traps: linkUp and linkDown

The following table describes the conditions that define linkUp and linkDown for each interface:

Interface	linkUp/Down Variable-Bindings	Possible Cause
Physical Sublayer – Represented by the entry in the MIB II Interfaces Table.		
DDS network (Supported by the media-specific DDS Enterprise MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ ifType (RFC 1573) ■ ddsStatus (DDS Enterprise MIB)	■ **linkDown** – One or more alarm conditions are active on the interface. Alarm conditions include: – No Signal – Out of Service – Out of Frame – Crossed Pair Detected – In-band Framing Error – Excessive Bipolar Violations (BPVs) ■ **linkUp** – No alarms on the interface.
Synchronous User Data Port (Supported by the media-specific RS232-Like MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ ifType (RFC 1573)	■ **linkDown** – The Alarm condition active on the interface is DTR Off. The DTR alarm condition only generates a linkUp/linkDown trap if the DTE supports the DTR lead. ■ **linkUp** – No alarm on the interface.

Traps: enterpriseSpecific

The enterpriseSpecific trap indicates that an enterprise-specific event has occurred. The Specific-trap field in the Trap PDU identifies the particular trap that occurred. The following table lists the enterprise specific traps supported by the unit:

Trap	What It Indicates	Possible Cause
enterpriseSelfTestFail(2)	A hardware failure of the unit is detected during the unit's self-test. The trap is generated after the unit completes initialization. There are no variable-bindings.	Failure of one or more of the unit's hardware components.
enterpriseDeviceFail(3)	An internal device failure. There are no variable-bindings.	Operating software has detected an internal device failure.
enterpriseTestStart(5)	A test is running.	At least one test has been started on an interface.
enterpriseConfigChange(6)	The configuration changed via the user interface or an SNMP manager. The trap is sent after 60 seconds have elapsed without another change. This suppresses the sending of numerous traps when multiple changes are made in a short period of time, as is typically the case when changing configuration options. There are no variable-bindings.	Configuration has been changed via the user interface or an SNMP manager.
enterpriseTestStop(105)	All tests have been halted.	All tests have been halted on an interface.

The tests that affect the enterpriseTestStart, enterpriseTestStop, and the variable-binding are different for each particular interface. Diagnostic tests are only supported on the physical DDS network and user data port interfaces. The specific tests and variable-bindings are described in the following table:

Interface	**enterpriseTestStart/Stop Variable-Bindings**	**Possible Cause**
Physical Sublayer		
DDS network	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ ifType (RFC 1573) ■ ddsTestType (DDS Enterprise MIB)	■ enterpriseTestStart – Any one of the following tests is active on the interface: – DSU Loopback – CSU Loopback – Send 511 pattern – Monitor 511 pattern ■ enterpriseTestStop – No longer has any tests running on the interface.
Synchronous User Data Ports	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ ifType (RFC 1573) ■ ifTestType (RFC 1573)	■ ifTestType – Any one of the following tests is active on the port: – Local Loopback (DTE) – Send 511 pattern – Monitor 511 pattern ■ ifTestType – No longer has any tests running on the port.

Cables and Pin Assignments

E

Overview

The following sections provide pin assignments for the:

- *Terminal Port (EIA-232) Connector*
- *DTE Port (V.35) Connector*
- *Standard EIA-232-D Crossover Cable*
- *Standard Null Modem Cable*
- *10BaseT Connector*
- *Modular RJ48S DDS Network Interface Connector*

Terminal Port (EIA-232) Connector

The Terminal port connects to a PC or VT100-compatible terminal.

Signal	Direction	Pin #
Transmit Data (TXD)	To DSU (In)	2
Received Data (RXD)	From DSU (Out)	3
Request to Send (RTS)	To DSU (In)	4
Clear to Send (CTS)	From DSU (Out)	5
Data Set Ready (DSR)	From DSU (Out)	6
Signal Ground (SG)	—	7
Carrier Detect (CD)	From DSU (Out)	8
Data Terminal Ready (DTR)	To DSU (In)	20

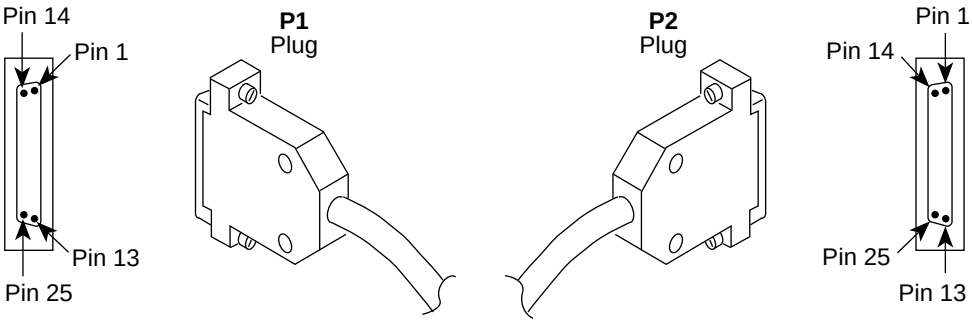
DTE Port (V.35) Connector

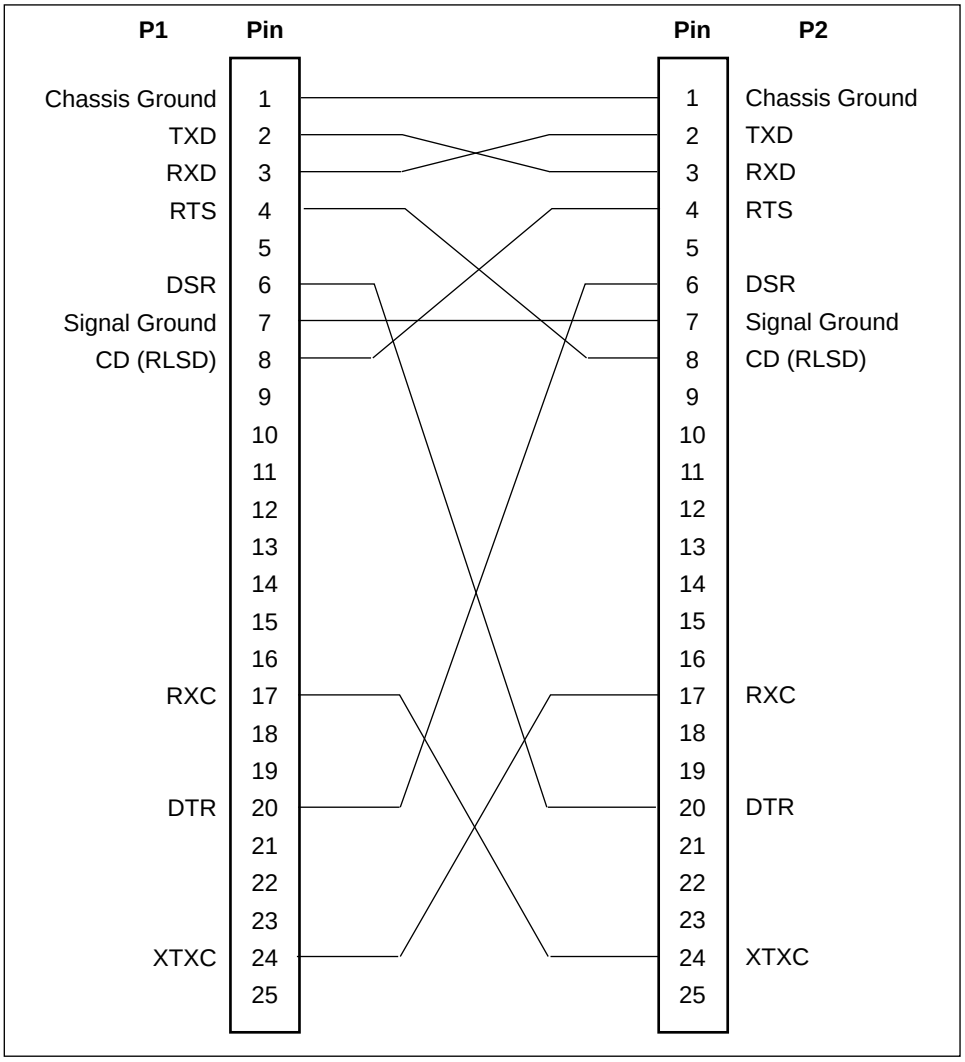
The following table provides the pin assignments for the 34-position V.35 connector to the user data terminal equipment.

Signal	ITU CT Number	Direction	34-Pin Socket Connector
Signal Ground/Common	102	—	B
Request to Send (RTS)	105	To DSU (In)	C
Clear to Send (CTS)	106	From DSU (Out)	D
Data Set Ready (DSR)	107	From DSU (Out)	E
Received Line Signal Detector (RLSD or LSD)	109	From DSU (Out)	F
Data Terminal Ready (DTR)	108/1, /2	To DSU (In)	H
Remote Loopback (RL)	140	To DSU (In)	N
Local Loopback (LL)	141	To DSU (In)	L
Transmitted Data (TXD)	103	To DSU (In)	P (A) S (B)
Received Data (RXD)	104	From DSU (Out)	R (A) T (B)
Transmitter Signal Element Timing — DTE Source (XTXC or TT)	113	To DSU (In)	U (A) W (B)
Receiver Signal Element Timing — DCE Source (RXC)	115	From DSU (Out)	V (A) X (B)
Transmitter Signal Element Timing — DCE Source (TXC)	114	From DSU (Out)	Y (A) AA (B)
Test Mode Indicator (TM)	142	From DSU (Out)	NN

Standard EIA-232-D Crossover Cable

A standard crossover cable can be used to connect the Terminal port to an external modem. This type of cable can be used for synchronous or asynchronous connections.

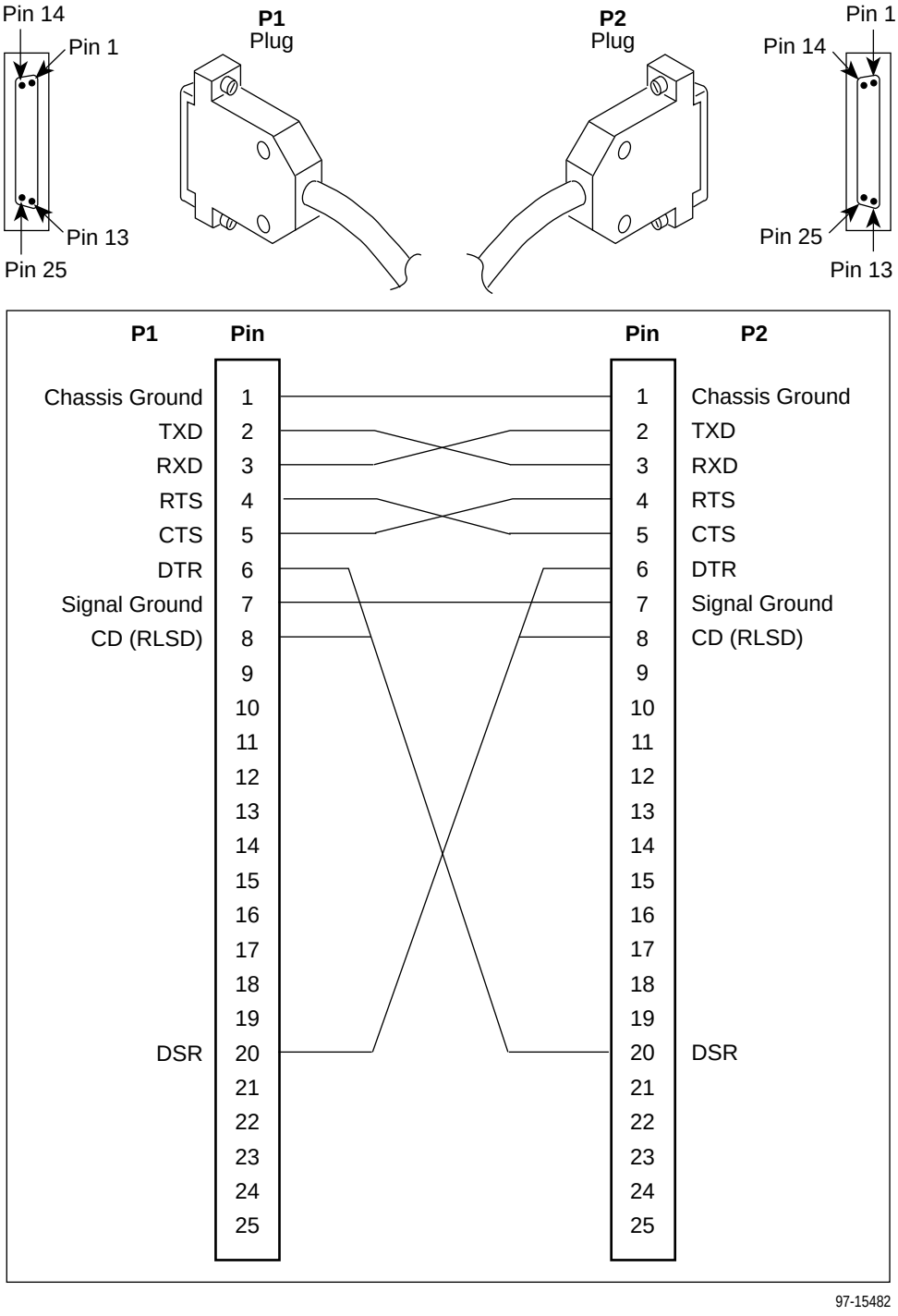




97-15180-01

Standard Null-Modem Cable

A standard null-modem cable can be used to connect the Terminal port to an external modem. This type of cable is used for asynchronous connections.



97-15482

10BaseT Connector

Use a standard 10BaseT cable to connect the DSU to an Ethernet LAN. A cable is provided with the DSU.

The following table defines the pinouts for the 10BaseT port. It is an 8-pin, unkeyed jack.

Use	Pin #
Transmitted Data +	1
Transmitted Data –	2
Received Data +	3
NC	4
NC	5
Received Data –	6
NC	7
NC	8
NC = Not connected (unused).	

Modular RJ48S DDS Network Interface Connector

Network access is via a modular cable with an RJ48S keyed plug connector on each end.

Use	Circuit	Pin #
Transmitted data to the local loop	R	1
Transmitted data to the local loop	T	2
NC	–	3
NC	–	4
NC	–	5
NC	–	6
Received data from the local loop	T1	7
Received data from the local loop	R1	8
NC = Not connected (unused).		

Technical Specifications

F

Table F-1. Model 7612 DSU Technical Specifications (1 of 2)

Item	Specifications
Housing	
Height (including feet)	2.1 inches (5.3 cm)
Height (without feet)	2.0 inches (5.1 cm)
Width	8.7 inches (22.1 cm)
Depth (case)	6.2 inches (15.7 cm)
Depth (case and connectors)	6.5 inches (16.5 mm)
Weight	1.3 pounds (0.6 kg)
Power	
Normal service voltage range	Input: 120 Vac ±12 Vac, 60 Hz ±3 Hz 4.9 watts (max.) at 120 Vac
Approvals	
FCC Part 15	Class A digital device
FCC Part 68	Refer to the equipment's label for Registration Number.
Safety Certifications	Refer to the equipment's label for approvals on product.
Industry Canada CS-03	Refer to the equipment's label for Certification Number.
Interface and Connector	
25-pin DB25 connector	EIA-232/ ITU V.24 (ISO 2110) for Terminal port
34-pin MS34 connector	ITU V.35 (ISO 2593) for DTE Port
8-pin modular jack	USOC RJ48S for Network port Unkeyed for 10BaseT port
Physical Environment	
Operating Temperature	32° to 122° F (0° to 50° C)
Storage Temperature	–4° to 158° F (–20° to 70° C)
Relative Humidity	5%—95% (noncondensing)
Shock and Vibration	Withstands normal shipping and handling

Table F-1. Model 7612 DSU Technical Specifications (2 of 2)

Item	Specifications
Heat Dissipation	11.6 Btu/hr. (max.) at 120 Vac
Network Interface	
Data rates	56 kbps and 64 kbps clear channel (CC)
LADS data rates	56 kbps and 64 kbps
Services supported	4-wire service
Terminal Port Data Rates	2.4, 4.8, 9.6, 14.4, 19.2, 28.8, and 38.4 kbps Defaults: 9.6 kbps with 8 bits per character, 1 stop bit, and no parity
Network Compatibility	
ANSI T1.410–1992 and AT&T Technical Reference 62310–1993	56 kbps and 64 kbps meeting desired loop loss
IP Connectivity	Up to 20 routes
NMS Compatibility	SNMP Network Manager
MIB II Object Groups Supported	■ ICMP group ■ Interfaces group: – DDS network – DTE Data port – Terminal port – Ethernet port ■ IP group ■ SNMP group ■ System group ■ TCP group ■ Transmission group: – DDS network – DDS Enterprise MIB – DTE Data port – RS-232-Like MIB – Terminal port – RS-232-Like MIB – 10BaseT port – Ethernet-Like MIB ■ UDP group

Table F-2. Model 7612 DTE Port Clock Rate

In-Band Management Channel (IMC) Rate	Line Operating Rate	
	56 Kbps	64 Kbps (CC or LADS)
0 (IMC disabled)	56,000 bps	64,000 bps
1,600 bps	54,400 bps	62,400 bps
4,000 bps	52,000 bps	60,000 bps
8,000 bps	48,000 bps	56,000 bps

Table F-3. Model 7612 DSU LADS Connection Distances

Data Rate (kbps)	Wire Diameter (AWG)			
	19 Gauge (.0359″ or .9122 mm)	22 Gauge (.0253″ or .643 mm)	24 Gauge (.0201″ or .511 mm)	26 Gauge (.0159″ or .404 mm)
56	10.84 mi (17.45 km)	6.4 mi (10.3 km)	4.50 mi (7.24 km)	3.34 mi (5.37 km)
64	10.69 mi (17.2 km)	6.06 mi (9.76 km)	4.47 mi (7.2 km)	3.20 mi (5.15 km)

Glossary

agent	A software program housed within a device to provide SNMP functionality. Each SNMP agent stores management information and responds to the manager's request.
aggregate	A single bit stream that combines two or more bit streams.
ASCII	American Standard Code for Information Interchange. A 7-bit code that establishes compatibility between data services. ASCII is the standard for data transmission over telephone lines.
asynchronous	A data transmission that is synchronized by a transmission start bit at the beginning of a character (five to eight bits) and one or more stop bits at the end.
ATI	ASCII Terminal Interface. This feature allows a device to be controlled from an asynchronous terminal or through a Telnet session.
autobaud mode	An operational mode in which the DSU forces automatic setting of the DDS line rate/speed (56 kbps or 64 kbps) as soon as a valid DDS network signal is detected.
BPV	Bipolar Violation. A modified bipolar signaling method in which a control code is inserted.
CCA	Circuit Card Assembly. A printed circuit board to which separate components are attached.
CCITT	Consultative Committee on International Telegraphy and Telephony. See ITU.
CD	Carrier Detect. A signal indicating that energy exists on the transmission circuit. Associated with Pin 8 on an EIA-232 interface.
channel	An independent data path.
CMI	Control Mode Idle. A control signal sent over the DDS line to indicate that no data is being sent.
COM port	Communications port. A computer's serial communications port used to transmit to and receive data.
configuration option	Device software that sets specific operating parameters for the DSU.
CPE	Customer Premises Equipment. Terminating equipment supplied by either the customer or some other supplier that is connected to the telecommunications network (e.g., DSUs, terminals, phones, routers, modems).
crossed pair	An alarm condition in which the DDS receive and transmit pairs are crossed.
CSU	Channel Service Unit. The function of the DSU that protects the equipment beyond it from damage due to disturbances on the DDS network, and regenerates the DDS signal to meet DDS specifications.
CTS	Clear to Send. An EIA-lead standard for V.24 circuit CT 106; an output signal (DCE-to-DTE).
DCE	Data Communications Equipment. The equipment that provides the functions required to establish, maintain, and end a connection. It also provides the signal conversion required for communication between the DTE and the network.
DDS	Digital Data Service. Provides digital communication circuits.
DMI	Data Mode Idle. Refers to a sequence of ones transmitted or received on the DDS network.

DSR	Data Set Ready. An EIA-lead standard for V.24 circuit CT 107; an output signal (DCE-to-DTE).
DSU	Data Service Unit. Data communications equipment that provides an interface between the DTE and the digital network.
DTE	Data Terminal Equipment. The equipment, such as computers and printers, that provides or creates data.
DTR	Data Terminal Ready. An EIA-lead standard for V.24 circuit CT 108; an input signal (DTE-to-DCE).
EIA	Electronic Industries Association. This organization provides standards for the data communications industry to ensure uniformity of interface between DTEs and DCEs.
EIA-232	The EIA's standards defining the 25-pin interface between the DTE and DCE.
Enterprise MIB	MIB objects unique to Paradyne devices.
excessive BPV	An excessive bipolar violation condition results when at least one invalid bipolar violation has occurred every 20 milliseconds for 2 seconds.
factory defaults	A predetermined set of configuration options for general operation.
FCC	Federal Communications Commission. Board of Commissioners that regulates all U.S. interstate, intrastate, and foreign electrical communication systems that originate from the United States.
frame relay	A switching interface that is designed to get frames from one part of the network to another as quickly as possible.
full-duplex	The capability to transmit in two directions simultaneously.
HDLC	High-Level Data Link Control. A communications protocol defined by the International Standards Organization (ISO).
ICMP	Internet Control Management Protocol. Internet protocol that allows for the generation of error messages, tests packets, and information messages related to IP.
IMC	In-band Management Channel. A proprietary TDM channel used for IP connectivity.
interface	A shared boundary between functional units.
IP	Internet Protocol. The TCP/IP standard protocol that defines the unit of information passed across an Internet and provides the basis for packet delivery service. IP includes the ICMP control and error message protocol as an integral part. The entire protocol suite is often referred to as TCP/IP because TCP and IP are the two most fundamental protocols.
IP address	The IP address has a host component and a network component. The address is assigned to hosts or workstations with direct Internet access to uniquely identify entities on the Internet.
ITU	International Telecommunication Union, formerly known as CCITT. An advisory committee established by the United Nations to recommend communications standards and policies.
LADS	Local Area Data Set is used to provide a point-to-point link between two devices (also called LDM – limited distance modem).
LAN	Local Area Network. A network designed to connect devices over short distances, like within a building.
latching loopback	A loopback that is maintained until a specific release code is detected. A latching loopback can only be initiated or terminated by the 64 kbps clear channel network service provider.
LED	Light Emitting Diode. A status indicator that responds to the presence of a certain conditions.

link layer protocol	The protocol that regulates the communication between two network nodes.
LL	Local Loopback. An EIA-lead standard for V.24 circuit CT 141; an input signal (DTE-to-DCE).
loopback	Used to test various portions of a data link in order to isolate an equipment or data line problem. A diagnostic procedure that sends a test message back to its origination point.
LSD	Line Signal Detect. An EIA-lead standard for V.24 circuit CT 109; an output signal (DCE-to-DTE).
manager (SNMP)	The device that queries agents for management information, or receives unsolicited SNMP trap messages indicating the occurrence of specific events.
MIB	Management Information Base. The set of variables a device running SNMP maintains. Standard, minimal MIBs have been defined, and vendors often have private enterprise MIBs. In theory, any SNMP manager can talk to any SNMP agent with a properly defined MIB. MIB-II refers to an extended management database that contains variables not defined in the original MIB I.
multiplexing	A method for interleaving several access channels onto a single circuit for transmission over the network.
NMS	Network Management System. A computer system used for monitoring and controlling network devices.
node	A connection or switching point on the network.
non-latching loopback	A loopback that is not maintained unless network loopback codes are interspersed with the test data. A non-latching loopback can only be initiated or terminated by the 56 kbps network service provider.
NS	No Signal. A network-reported condition.
object (SNMP)	A specific item within the Management Information Base (MIB).
OOF	Out Of Frame. An error condition in which frame synchronization bits are in error. A network-reported condition.
OOS	Out of Service. A digital network trouble signal.
PAD	Packet Assembler/Disassembler.
point-to-point circuit	A data network circuit with one control and one tributary device.
PPP	Point-to-Point Protocol. A link-layer protocol used by SNMP.
protocol	The rules that govern how devices exchange information on a network. It covers timing, format, error control, and flow control during data transmission.
PSTN	Public Switched Telephone Network. A network shared among many users who can use telephones to establish connections between two points.
reset	A reinitialization of the device that occurs at power-up or in response to a reset command.
RFC	Request for Comments. The set of documents that describes the standard specifications for the TCP/IP protocol suite.
RIP	Routing Information Protocol. Specifies the routing protocol used between DSUs.
RLSD	Receive Line Signal Detect. See CD.
router	A device that makes decisions about the paths network traffic should take and forwards that traffic to its destination. A router helps achieve interoperability and connectivity between different vendor's equipment, regardless of protocols used.

RS-232 An EIA standard for the 25-pin DCE/DTE interface. Same as EIA-232.

RTS Request to Send. An EIA-lead standard for V.24 circuit CT 105; an input signal (DTE-to-DCE).

RXC Received Clock. An EIA-lead standard for V.24 circuit CT 115; an output signal (DCE-to-DTE).

RXD Received Data. An EIA-lead standard for V.24 circuit CT 104; an output signal (DCE-to-DTE).

SDLC Synchronous Data Link Control. A standard data link protocol.

SNMP Simple Network Management Protocol. A generic internet network management protocol that allows the device to be managed by any industry-standard SNMP manager.

subnet An IP addressing standard in which a portion of the host address can be used to create multiple network addresses that are logically a subdivision of the network address.

subnet address The subnet portion of an IP address. In a subnetted network, the host portion of an IP address is split into a subnet portion and a host portion using a subnet address mask. This allows a site to use a single IP network address for multiple physical networks.

subnet mask An integer used with the IP address of the host to determine which bits in the host address are used in the subnet address.

synchronous Data transmission that is synchronized by timing signals. Characters are sent at a fixed rate.

TCP/IP Transmission Control Protocol/Internet Protocol. Refer to IP.

TDM Time Division Multiplexer. A device that enables the simultaneous transmission of multiple independent data streams into a single high-speed data stream.

Telnet Virtual terminal protocol in the Internet suite of protocols. Allows the user of one host computer to log into a remote host computer and interact as the user for that host.

TM Test Mode. An EIA-lead standard for V.24 circuit CT 142; an output signal (DCE-to-DTE).

TXC Transmit Clock. An EIA-lead standard for V.24 circuit CT 114; an output signal (DCE-to-DTE).

TXD Transmit Data. An EIA-lead standard for V.24 circuit CT 103; an input signal (DTE-to-DCE).

UDP User Datagram Protocol. An Internet protocol.

V.35 ITU-T standard for a high-speed, 34-pin, DCE/DTE interface.

WAN Wide Area Network. A network that operates over long distances and spans a relatively large geographic area (e.g., a country).

Index

Numbers

10BaseT cable, E-6
10BaseT port. *See* Ethernet port
511 test pattern, 7-4

A

access
  effective level, 4-3
  SNMP, 4-6, A-14
  Telnet session, A-13
  to the ATI, 4-1
administer login, 4-2
alarm
  condition, 7-1
  LED, 6-3
ASCII
  alarm, 7-1
  printable characters, 3-1
ATI
  access, 4-3
  initiating, 2-1
  management, 1-1
  monitoring, 6-1

C

cables
  crossover, E-4
  DDS network, E-6
  DTE (V.35), E-3
  EIA–232, E-2
  Ethernet, E-6
  null modem, E-5
  rear panel, E-1
cables to order. *See* Startup Instructions
Carrier Control by RTS, A-8
Clear command, 6-6
clock rates, F-3
clocking, inversion, A-7
ClrStats command, 6-6
community names, for SNMP, 4-6
configuration
  menu, 2-2
  option areas, 3-4
  option tables, A-1
  option worksheets, B-1
configuration examples, 1-3
connectors
  10BaseT port, E-6
  DTE port (V.35), E-3
  Network port, E-6
  rear panel, E-1
  Terminal port, E-2
control, menu, 2-2
create login ID, 4-2
crossover EIA-232 cable, E-4
CTS
  clear to send LED, 6-5
  control, A-8
customer, configuration areas, 3-4

D

data port
  options, A-7
  tests, 7-5
data scrambling, A-5
DDS
  line rate, A-3
  operating mode, A-2
defaults
  configuration option, 3-4
  reload factory, 7-8
device
  messages, 8-2
  name, 3-1
  reset, 7-8
Disconnect Time, A-12
displaying, configuration options, 3-5
DM, data mode LED, 6-4
DSR Control, A-8
DTE port
  clock rates, F-3
  options, A-7

DTE test, 7-5
DTR
  action, A-9
  data terminal ready LED, 6-5
  monitoring, A-11

E

effective access
  and screen contents, 2-3
  to ATI, 4-3
EIA-232 pin assignments, E-2
Enterprise MIB
  objects supported, C-17
  SNMP traps, D-3
Ethernet cable, E-6
Ethernet port
  connector, E-6
  default gateway address, A-10
  IP address, A-9
  IP subnet mask, A-10
  options, A-9
  Use, A-9
Ethernet-Like MIB
  objects not supported, C-17
  objects supported, C-17
external device, access, 4-1

F

factory defaults, for configuration options, 3-4
features, 1-1

G

glossary, GL-1–GL-4

H

health and status, messages, 6-6

I

identity, 3-1
IMC
  access, 4-1
  IP address, A-6
  rate, A-5
  remote management, 1-1
  Routing Information Protocol, A-6
  subnet connection, 5-2
  subnet mask, A-6
Inactivity Timeout, A-12
installing rear connectors. *See* Startup Instructions
interface
  connections, 1-4
  network status, 6-10
invert transmit clock, A-7
IP address
  Ethernet port, A-9
  IMC, A-6
  NMS, A-16
  scheme, 5-1
  SNMP manager, 4-6
  trap manager, A-17
IP interfaces, 4-1, 5-2

K

keyboard functions, 2-5

L

LADS
  connection distances, F-3
  line rate, A-3
  operating mode, A-2
  timing, A-3
lamp test, 7-6
LAN adapter, addressing, 5-1
LAN cable, E-6
LEDs, 6-2
link-layer protocols, 5-1
login
  required for Terminal port, A-11
  required for Telnet session, A-13

login ID, 4-1
loopback
  bilateral, A-7
  DTE–initiated, A-7
  network–initiated, A-5
  V.54–initiated, A-5
loopbacks, 7-3

M

main menu
  configuration options, A-1
  tree structure, 2-2
management, of SNMP DSU, 1-1
Management Protocol Statistics, 6-13
messages
  alarm and device, 8-1
  health and status, 6-6
  self-test results, 6-8
  test status, 6-9
MIB
  descriptions, C-1
  Enterprise MIB objects supported, C-17
  Ethernet–Like MIB objects supported, C-17
  general support, 1-4
  MIB II objects not supported, C-2
  MIB II objects supported, C-1
  RS–232–Like MIB object groups supported, C-13
MIB II
  Extension to Interface Table, C-6
  Generic Receive Address Table, C-9
  ICMP Group, C-12
  Interface Stack Group, C-7
  Interface Test Table, C-8
  Interfaces Group, C-3
  IP Group, C-10
  SNMP Group, C-12
  SNMP traps, D-2
  System Group, C-2
  TCP Group, C-12
  Transmission Group, C-12
  UDP Group, C-12
Monitor DTR, A-11

N

navigating the screens, 2-5
network
  interface cable, E-6
  interface LEDs, 6-4
  interface options, A-5
  interface status, 6-10
  loopbacks, 7-3
  performance statistics, 6-11
  tests, 7-3
NMS
  IP validation, A-15
  SNMP access, 4-6
  SNMP connectivity, 5-1
  SNMP security options, A-15
NS, no signal LED, 6-4
null modem cable, E-5

O

objects for MIBs, C-1
OK, LED, 6-3
OOF, out of frame LED, 6-4
OOS, out of service LED, 6-4
operating mode, A-2
options
  configuration areas, 3-4
  configuration tables, A-1
  configuration worksheets, B-1

P

package checklist. *See* Startup Instructions
performance, network statistics, 6-11
pin assignments, E-1
port
  access, 4-1
  LEDs, 6-5

R

rear panel, connections, 1-4
Refresh command, 6-6
reset device, 7-8
RFC 1213, object groups supported, C-1
RFC 1573, object groups supported, C-1
RFC 1643, object groups supported, C-17
RFC 1659, object groups supported, C-13
RIP option, 5-1
RJ48S network interface cable, E-6
RLSD Control, A-8
router, management data, 5-3
RS–232–Like MIB
  Asynchronous Port Table Objects, C-14
  General Port Table Objects, C-13
  Input Signal Table Objects, C-16
  Number of RS–232–Like Ports, C-13
  objects supported, C-13
  Output Signal Table Objects, C-17
  Synchronous Port Table Objects, C-15
RTS
  action, A-8
  request to send LED, 6-5
RXD, received data LED, 6-5

S

safety instructions. *See* Startup Instructions
saving option changes, 3-6
screens, for user interface, 2-1
security, 4-1
self-test results, 6-8
session, Telnet access, 4-1
SNMP
  Community Name, A-14
  number of managers, A-15
  number of trap managers, A-17
  security, A-15
  system entries, 3-1
  trap types generated, A-18
  traps, 8-1, A-17, D-1
SNMP management
  general, 1-4
  limiting access, 4-6
  options, A-14
startup, ATI, 2-1
startup instructions. *See* Startup Instructions
statistics
  Management Protocol, 6-13
  Network Performance, 6-11
status
  DSU, 6-6
  menu, 2-2
  network interface, 6-10
  test messages, 6-9
subnet, IP addresses, 5-1
system
  device name fields, 3-1
  LEDs, 6-3

T

technical specifications, F-1
Telnet session
  access, 4-1
  access level, A-13
  Disconnect Time, A-13
  options, A-12
  timeout, A-13
  to initiate ATI, 2-1
Terminal port
  access level, A-11
  character length, A-10
  data rate, A-10
  direct connection, 2-1
  login, A-11
  options, A-10
  parity, A-11
  reset, 7-8
  stop bits, A-11
terminal port, access, 4-1
test
  DTE, 7-5
  LED, 6-3
  menu, 2-2
  network, 7-3
  status messages, 6-9
Test Duration, A-4
Test Timeout, A-4
testing, 7-1
timeout
  Telnet session inactivity, A-13
  Terminal port inactivity, A-12

Trap Manager
destination, A-17
IP address, A-17
number, A-17
traps, SNMP, 8-1, D-1
troubleshooting, 8-3
TXD, transmitted data LED, 6-5

U

user interface
access, 2-1
async terminal, 2-1

V

V.35 connector, E-3
V.54 sequences, 7-4
VT100 compatible terminal. *See* ATI

W

worksheets, option configuration, B-1